No. 17-2

In the Supreme Court of the United States

UNITED STATES OF AMERICA, PETITIONER

v.

MICROSOFT CORPORATION

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

JOINT APPENDIX

NOEL J. FRANCISCO
Solicitor General
Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

Counsel of Record
for Petitioner

E. JOSHUA ROSENKRANZ
Orrick, Herrington &
Sutcliffe, LLP
51 West 52nd Street
New York, NY 10019
jrosenkranz@orrick.com
(212) 506-5000

Counsel of Record
for Respondent

PETITION FOR A WRIT OF CERTIORARI FILED: JUNE 23, 2017
CERTIORARI GRANTED: OCT. 16, 2017

TABLE OF CONTENTS

Page

Court of appeals docket entries 1
District court docket entries 8
Redacted warrant (Dec. 4, 2013) 22
Stipulation regarding contempt order (Sept. 8, 2014) 27
Declaration of [Redacted] (Apr. 25, 2014) 29
Declaration of [Redacted] (Apr. 25, 2014) 33
Declaration of [Redacted] (June 6, 2014) 36
Declaration of Rajesh Jha (June 5, 2014) 39
Declaration of Michael McDowell (June 6, 2014) 47
Declaration of Claire Catalano (June 6, 2014) 51
Exhibit 1: Email from Christopher B. Harwood, Assistant United States Attorney, United States Attorney's Office for the Southern District of New York, to Nathan Wessler, American Civil Liberties Union (Apr. 19, 2013 16:59 PM) 53
Exhibit 3: Letter from Sophie in't Veld, Member, European Parliament, to Viviane Reding, Vice-President, European Commission (Apr. 28, 2014) 56
Supplemental Declaration of Claire Catalano (July 24, 2014) 59
Exhibit 1: Letter from Viviane Reding, Vice-President, European Commission, to Sophie in't Veld, Member, European Parliament (June 24, 2014) 63
Exhibit 2: Christian Kahle, *US Wants to Rule over All Servers Globally* (July 25, 2014) 67
Exhibit 3: Franceso Lanza, *US Government to Microsoft: "Data stored online are not protected under the Fourth Amendment"* (July 15, 2014) 71

Table of Contents—Continued: Page

Exhibit 4: *US Government: Microsoft Servers Subject to US Laws, Irrespective of Country* (July 15, 2014) 75
Exhibit 5: Henning Steier, *US Government Accessing Data on Foreign Servers* (July 15, 2014) 79
Exhibit 6: *Obama also demands access to data stored outside US* (July 15, 2014) 84
Exhibit 7: *Obama Also Requires Access to Data Stored Outside of the USA* (July 15, 2014) 88
Exhibit 8: *US Government Requests Access to Data Held Abroad* (July 15, 2014) 92
Exhibit 9: *US Government: Access to Foreign Servers is Lawful* (July 15, 2014) 96
Exhibit 10: *US Government Requests Access to Data in EU Processing Centers* (July 15, 2014) 100
Exhibit 11: *US Also Wants Data from Foreign Servers* (July 15, 2014) 104
Exhibit 12: Richard Waters, *EU slams US over Microsoft privacy case* (June 30, 2014) 108
Declaration of Joseph V. DeMarco 112
Supplemental Declaration of Michael McDowell 121
Transcript of hearing before the Honorable Loretta A. Preska, United States District Judge (excerpts) (July 31, 2014) 124
Transcript of Second Circuit oral argument (excerpts) (Sept. 9, 2015) 135

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

Docket No. 14-2985

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

MICROSOFT CORPORATION, APPELLANT

v.

UNITED STATES OF AMERICA, APPELLEE

DOCKET ENTRIES

DATE	DOCKET NUMBER	PROCEEDINGS
8/12/14	1	NOTICE OF CIVIL APPEAL, with district court docket, on behalf of Appellant In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation, FILED. [1300731] [14-2985] [Entered: 08/21/2014 10:23 AM]
		* * * * *
9/10/14	33	AMENDED NOTICE OF APPEAL, with copy of district court docket, on behalf of Appellant Microsoft Corporation, FILED.

DATE	DOCKET NUMBER	PROCEEDINGS
		[1317066] [14-2985] [Entered: 09/11/2014 08:50 AM]
		* * * * *
12/8/14	47	BRIEF, on behalf of Appellant Microsoft Corporation, FILED. Service date 12/08/2014 by CM/ECF. [1387372] [14-2985] [Entered: 12/08/2014 12:54 PM]
12/8/14	48	SPECIAL APPENDIX, on behalf of Appellant Microsoft Corporation, FILED. Service date 12/08/2014 by CM/ECF. [1387385] [14-2985] [Entered: 12/08/2014 12:58 PM]
12/8/14	49	JOINT APPENDIX, volume 1 of 2, (pp. 1-144), on behalf of Appellant Microsoft Corporation, FILED. Service date 12/08/2014 by CM/ECF. [1387399] [14-2985] [Entered: 12/08/2014 01:08 PM]
12/8/14	50	JOINT APPENDIX, volume 2 of 2, (pp. 145-346), on behalf of Appellant Microsoft Corporation, FILED. Service date 12/08/2014 by CM/ECF. [1387414] [14-2985] [Entered: 12/08/2014 01:15 PM]
		* * * * *
3/9/15	212	BRIEF, on behalf of Appellee United States of America, FILED.

DATE	DOCKET NUMBER	PROCEEDINGS
		Service date 03/09/2015 by 3rd party, CM/ECF. [1456279] [14-2985] [Entered: 03/09/2015 08:56 PM]
		* * * * *
4/8/15	222	REPLY BRIEF, on behalf of Appellant Microsoft Corporation, FILED. Service date 04/08/2015 by CM/ECF. [1480496] [14-2985] [Entered: 04/08/2015 08:07 PM]
		* * * * *
9/9/15	246	CASE, before GEL, SLC, C.JJ., BOLDEN, D.J., HEARD. [1594176] [14-2985] [Entered: 09/09/2015 01:27 PM]
		* * * * *
10/6/15	255	FRAP 28(j) LETTER, dated 10/06/2015, on behalf of Appellant Microsoft Corporation, RECEIVED. Service date 10/06/2015 by CM/ECF. [1614227] [14-2985] [Entered: 10/06/2015 05:32 PM]
		* * * * *
10/17/15	259	FRAP 28(j) LETTER, dated 10/17/2015, on behalf of Appellee United States of America, RECEIVED. Service date 10/17/2015

DATE	DOCKET NUMBER	PROCEEDINGS
		by CM/ECF. [1621580] [14-2985] [Entered: 10/17/2015 11:46 AM]
		* * * * *
4/15/16	269	FRAP 28(j) LETTER, dated 04/15/2016, on behalf of Appellant Microsoft Corporation, RECEIVED. Service date 04/15/2016 by CM/ECF. [1752087] [14-2985] [Entered: 04/15/2016 05:09 PM]
5/25/16	271	FRAP 28(j) LETTER, dated 05/25/2016, on behalf of Appellee United States of America, RECEIVED. Service date 05/25/2016 by CM/ECF. [1780401] [14-2985] [Entered: 05/25/2016 11:16 PM]
		* * * * *
7/14/16	286	OPINION, reversing the District Court's denial of Microsoft's motion to quash and vacating its order holding Microsoft in civil contempt of court and remanding the case with instructions to quash the warrant insofar as it demands user content stored outside of the United States, by GEL, SLC, V.A. BOLDEN, FILED. [1815361] [14-2985] [Entered: 07/14/2016 10:30 AM]

DATE	DOCKET NUMBER	PROCEEDINGS
7/14/16	287	OPINION, Concurring, by judge GEL, FILED. [1815366] [14-2985] [Entered: 07/14/2016 10:32 AM]
7/14/16	288	CERTIFIED OPINION, dated 07/14/2016, to SDNY (NEW YORK CITY), ISSUED. [1815374] [14-2985] [Entered: 07/14/2016 10:37 AM]
7/14/16	292	JUDGMENT, FILED. [1816057] [14-2985] [Entered: 07/14/2016 04:21 PM]
7/15/16	294	INTERNET CITATION NOTE: Material from decision with internet citation, ATTACHED. [1817355] [14-2985] [Entered: 07/15/2016 04:51 PM]
		* * * * *
10/13/16	316	PETITION FOR REHEARING/ REHEARING EN BANC, on behalf of Appellee United States of America, FILED. Service date 10/13/2016 by CM/ECF. [1883945] [14-2985] [Entered: 10/13/2016 07:19 PM]
		* * * * *
1/24/17	327	ORDER, petition for rehearing en banc denied, FILED. [1953043]

DATE	DOCKET NUMBER	PROCEEDINGS
		[14-2985] [Entered: 01/24/2017 09:14 AM]
1/24/17	328	OPINION, Concurring, by Judge SLC, FILED. [1953056] [14-2985] [Entered: 01/24/2017 09:18 AM]
1/24/17	329	OPINION, Dissenting, by Judge DJ, FILED. [1953062] [14-2985] [Entered: 01/24/2017 09:19 AM]
1/24/17	330	OPINION, Dissenting, by Judge JAC, FILED. [1953069] [14-2985] [Entered: 01/24/2017 09:20 AM]
1/24/17	331	OPINION, Dissenting, by Judge RR, FILED. [1953075] [14-2985] [Entered: 01/24/2017 09:22 AM]
1/24/17	332	OPINION, Dissenting, by Judge CFD, FILED. [1953082] [14-2985] [Entered: 01/24/2017 09:23 AM]
1/24/17	335	INTERNET CITATION NOTE: Material from decision with internet citation, ATTACHED. [1955745] [14-2985] [Entered: 01/26/2017 02:41 PM]
1/24/17	336	INTERNET CITATION NOTE: Material from decision with internet citation, ATTACHED. [1955747] [14-2985] [Entered: 01/26/2017 02:41 PM]

DATE	DOCKET NUMBER	PROCEEDINGS
2/1/17	337	JUDGMENT MANDATE, ISSUED. [1959572] [14-2985] [Entered: 02/01/2017 11:25 AM]

* * * * *

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Docket No. 1:13-mj-02814-UA-1

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

UNITED STATES OF AMERICA, PLAINTIFF

v.

MICROSOFT CORPORATION, DEFENDANT

DOCKET ENTRIES

DATE	DOCKET NUMBER	PROCEEDINGS
12/4/13	1	SEALED DOCUMENT placed in vault. So Ordered U.S. Magistrate Judge Michael H. Dolinger (Sealed Envelope is Document No. 14 under M9-150) (vb) (Entered: 05/29/2014)
1/30/14	2	SEALED DOCUMENT placed in vault. So Ordered U.S. Magistrate Judge James C. Francis IV (Sealed Envelope is Document No. 31 under M9-150) (vb) (Entered: 05/29/2014)
2/24/14	3	SEALED DOCUMENT placed in vault. So Ordered U.S. Magistrate Judge James C. Francis IV (Sealed

DATE	DOCKET NUMBER	PROCEEDINGS
		Envelope is Document No. 42 under M9-150) (vb) (Entered: 05/29/2014)
3/14/14	4	SEALED DOCUMENT placed in vault. So Ordered U.S. Magistrate Judge Frank Maas. (Sealed Envelope is Document No. 65 under M9-150) (vb) (Entered: 05/29/2014)
4/25/14	5	MEMORANDUM AND ORDER as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation denying Microsoft's motion to quash the warrant in part. (Signed by Magistrate Judge James C. Francis on 4/25/14) (Filed as Document no. 93 in case M9-150) (vb) (Entered: 05/29/2014)
4/25/14	6	REDACTED MEMORANDUM OF LAW by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation in Support Of Microsoft's Motion to Vacate in part an SCA warrant seeking customer information located outside the U.S.. (Filed as Document no. 94 in case M9-150) (vb) (Entered: 05/30/2014)

DATE	DOCKET NUMBER	PROCEEDINGS
4/25/14	7	REDACTED DECLARATION as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation in Support. (Filed as Document no. 95 in case M9-150) (vb) (Entered: 05/30/2014)
4/25/14	8	REDACTED DECLARATION as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation in Support. (Filed as Document no. 96 in case M9-150) (vb) (Entered: 05/30/2014)
4/25/14	9	MEMORANDUM OF LAW by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation in Opposition. (Filed as Document no. 97 in case M9-150) (vb) (Entered: 05/30/2014)
4/25/14	10	REDACTED REPLY MEMORANDUM OF LAW by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation in Support of Microsoft's Motion to Vacate in part an SCA

DATE	DOCKET NUMBER	PROCEEDINGS
		warrant seeking customer information located outside the U.S.. (Filed as Document no. 98 in case M9-150) (vb) (Entered: 05/30/2014)
		* * * * *
5/5/14	11	ENDORSED LETTER as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Magistrate Judge James C. Francis IV from Guy Petrillo dated 4/30/14 re: Microsoft respectfully seeks a stay of the Order pending appeal. ENDORSEMENT: Application granted. (Signed by Magistrate Judge James C. Francis on 5/5/14) (Filed as Document no. 109 in case M9-150) (vb). (Entered: 05/30/2014)
5/6/14	12	LETTER by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Magistrate Judge James C. Francis IV from AUSA Lorin L. Reisner dated 5/2/14 re: In response to the April

DATE	DOCKET NUMBER	PROCEEDINGS
		30, 2014 letter submitted by Microsoft Corp. requesting a stay pending appeal of the oder denying Microsoft's motion to vacate. The Government is prepared to consent to a stay on the condition that Microsoft seeks its appeal promptly and without any delay, so that this matter may proceed through the appropriate appeals process expeditiously Document filed by USA. (Filed as Document no. 114 in case M9-150) (vb) (Entered: 05/30/2014)
		* * * * *
6/6/14	15	Objections filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: 5 Order, denying Microsoft's Motion to Vacate in part a Search Warrant seeking customer information located outside the United States. (vb) (Entered: 06/09/2014)
6/6/14	16	DECLARATION filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (vb) (Entered: 06/09/2014)

DATE	DOCKET NUMBER	PROCEEDINGS
6/6/14	17	DECLARATION of Rajesh Jha filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (vb) (Entered: 06/09/2014)
6/6/14	18	DECLARATION of Michael McDowell filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (vb) (Entered: 06/09/2014)
6/6/14	19	SUPPLEMENTAL DECLARATION filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation supplementing the Declaration of December 17, 2013. (vb) (Entered: 06/09/2014)
6/6/14	20	DECLARATION of Claire Catalano in Support of the referenced motion, filed as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (vb) (Entered: 06/09/2014)
6/6/14	21	Certificate of Service of 18 Declaration, 20 Declaration in Support,

DATE	DOCKET NUMBER	PROCEEDINGS
		19 Declaration, 17 Declaration, 15 Reply, 16 Declaration filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. Document was served on AUSA Justin Anderson on 6/6/14. (vb) (Entered: 06/09/2014)
		* * * * *
7/9/14	60	MEMORANDUM in Opposition by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re 24 MOTION to File Amicus Brief by Jeffrey A. Novack.. (Anderson, Justin) (Entered: 07/09/2014)
		* * * * *
7/24/14	70	REPLY by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: 15 Reply, filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Kestenbaum, Nancy) (Entered: 07/24/2014)

DATE	DOCKET NUMBER	PROCEEDINGS
7/24/14	71	DECLARATION of Claire Catalano in Support as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: 70 Reply,. (Attachments: # 1 Exhibit 1, # 2 Exhibit 2, # 3 Exhibit 3, # 4 Exhibit 4, # 5 Exhibit 5, # 6 Exhibit 6, # 7 Exhibit 7, # 8 Exhibit 8, # 9 Exhibit 9, # 10 Exhibit 10, # 11 Exhibit 11, # 12 Exhibit 12, # 13 Exhibit 13, # 14 Exhibit 14, # 15 Exhibit 15) (Kestenbaum, Nancy) (Entered: 07/24/2014)
7/24/14	72	DECLARATION of Joseph V. DeMarco in Support as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: 70 Reply,. (Kestenbaum, Nancy) (Entered: 07/24/2014)
7/24/14	73	DECLARATION of Michael McDowell in Support as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: 70 Reply,. (Kestenbaum, Nancy) (Entered: 07/24/2014)

DATE	DOCKET NUMBER	PROCEEDINGS
		* * * * *
7/30/14	77	ORDER that the oral argument scheduled for July 31, 2014 at 10:30 a.m. shall be held in courtroom 26A of the U.S. Courthouse, 500 Pearl Street, New York, New York as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Signed by Judge Loretta A. Preska on 7/30/14) (vb) (Entered: 07/30/2014)
		* * * * *
7/31/14	78	LETTER by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Judge Loretta A. Preska from AUSA Serrin Turner dated 07/31/2014 re: stay pending appeal Document filed by USA. (Turner, Serrin) (Entered: 07/31/2014)
7/31/14		MEMORANDUM TO THE DOCKET CLERK: as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Cor-

DATE	DOCKET NUMBER	PROCEEDINGS
		poration. The Magistrate's decision is affirmed for the reasons set forth on the record at oral argument. So Ordered U.S.D.J. Loretta A. Preska. (vb) (Entered: 08/06/2014)
8/1/14	79	ENDORSED LETTER as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Judge Loretta A. Preska from Serrin Turner dated July 31, 2014 re: Giving notice of the governments consent to a stay of the courts decision pending an appeal. ENDORSEMENT: The Stay shall extend only for such period as will permit Microsoft to file its notice of appeal, request for a stay and request for an expedited appeal. (Signed by Judge Loretta A. Preska on 8/1/14) (vb) (Entered: 08/01/2014)
8/11/14	80	ORDER as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. This Order confirms that immediately

DATE	DOCKET NUMBER	PROCEEDINGS
		following oral argument on July 31, 2014, for the reasons set forth on the record, the Court affirms the decision of Magistrate Judge James C. Francis IV re: 5 Order, dated April 25, 2014. (Signed by Judge Loretta A. Preska on 8/11/14) (vb) (Entered: 08/12/2014)
8/11/14	81	NOTICE OF APPEAL by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation from 80 Order, 5 Order,. Filing fee $505.00, receipt number 465401102180. (nd) (Entered: 08/12/2014)
		* * * * *
8/12/14	82	LETTER MOTION addressed to Judge Loretta A. Preska from Justin Anderson and Serrin Turner dated August 12, 2014 re: Vacatur of Stay and Enforcement of Order. Document filed by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Anderson, Justin) (Entered: 08/12/2014)
		* * * * *

DATE	DOCKET NUMBER	PROCEEDINGS
8/19/14	87	LETTER RESPONSE to Motion by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Judge Loretta A. Preska from James M. Garland dated August 19, 2014 re: 82 LETTER MOTION addressed to Judge Loretta A. Preska from Justin Anderson and Serrin Turner dated August 12, 2014 re: Vacatur of Stay and Enforcement of Order . . (Garland, James) (Entered: 08/19/2014)
8/20/14	88	LETTER RESPONSE in Support of Motion by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Judge Loretta A. Preska from Justin Anderson and Serrin Turner dated 8/20/14 re: 82 LETTER MOTION addressed to Judge Loretta A. Preska from Justin Anderson and Serrin Turner dated August 12, 2014 re: Vacatur of Stay and Enforcement of Order . . (Anderson, Justin) (Entered: 08/20/2014)

DATE	DOCKET NUMBER	PROCEEDINGS
		* * * * *
8/29/14	90	MEMORANDUM AND ORDER granting 82 LETTER MOTION to lift the stay in execution of the Court's July 31, 2014 order as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation (1). (Signed by Judge Loretta A. Preska on 8/29/2014) (gq) (Entered: 08/29/2014)
9/4/14	91	**FILING ERROR—ELECTRONIC FILING OF NON-ECF DOCUMENT—** RESPONSE by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: 90 Order on Letter Motion, *Joint Stipulation and Proposed Order.* (Anderson, Justin) Modified on 9/5/2014 (ka). (Entered: 09/04/2014)
		* * * * *
9/8/14	92	STIPULATION AND ORDER as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. This Court

DATE	DOCKET NUMBER	PROCEEDINGS
		holds Microsoft Corporation in contempt for not complying in full with the warrant, and imposes no other sanctions at this time. The Government may seek sanctions in the case of materially changed circumstances in the underlying criminal investigation, or the second circuits issuance of the mandate in the appeal, if this court's order is affirmed and Microsoft continues not to comply with it. (Signed by Judge Loretta A. Preska on 9/8/14) (vb) (Entered: 09/08/2014)
		* * * * *
9/9/14	95	AMENDED NOTICE OF APPEAL by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation from 80 Order, 92 Stipulation and Order,,. (nd) (Entered: 09/09/2014)
		* * * * *

UNITED STATES DISTRICT COURT

for the

Southern District of New York

13 MAG 2814

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation

Case No.

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the WESTERN District of WASHINGTON
(identify the person or describe the property to be searched and give its location):
The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation (see attachments).

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See attachments.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before December 18, 2013
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.

✓ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court. JCF
USMJ Initials

☑ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☑ for 30 days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: December 4, 2013 4:32 pm

James C. Francis IV
Judge's signature

City and state: New York, NY

Hon. James C. Francis IV, Magistrate Judge, SDNY
Printed name and title

ATTACHMENT A

Property To Be Searched

This warrant applies to information associated with [redacted]@msn.com, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at One Microsoft Way, Redmond, WA 98052.

ATTACHMENT C

Particular Things To Be Seized

I. Information To Be Disclosed By MSN [redacted]:

To the extent that the information described in Attachment A for MSN, [redacted], is within the possession, custody, or control of MSN [redacted], then MSN [redacted] is required to disclose the following information to the Government for each account or identifier listed in Attachment A [redacted] (the "TARGET ACCOUNT") for the period of inception of the account to the present:

a. The contents of all e-mails stored in the account, including copies of e-mails sent from the account;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files,

and means and sources of payment (including any credit or bank account number);

c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

d. All records pertaining to communications between MSN [redacted] and any person regarding the account, including contacts with support services and records of actions taken.

II. Information To Be Seized By The Government

A variety of techniques may be employed to search the seized e-mails for evidence of the specified crimes, including but not limited to keyword searches for various names and terms including the TARGET SUBJECTS, and other search names and terms; and email-by-email review.

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 21, United States Code, Sections 846, 959, 960, and 963, Title 46, United States Code, Section 70503, and Title 18, United States Code, Section 1956, including, for each account or identifier listed on Attachment A [redacted], information pertaining to the following matters:

a. Any communications:

1. Pertaining to narcotics, narcotics trafficking, importation of narcotics into the United States, money laundering, or the movement or distribution of narcotics proceeds;

2. [redacted]

3. Pertaining to the use of ports or other places of entry to receive or ship narcotics or narcotics proceeds;

4. Related to the physical location of the TARGET SUBJECTS and their co-conspirators;

5. Constituting evidence of who uses the TARGET ACCOUNT, and where they live and work, and where they are using the TARGET ACCOUNT; and

6. Constituting information relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Case Nos. 13-MAG-2814; M9-150

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLELD AND MAINTAINED BY MICROSOFT CORPORATION

[Filed: Sept. 8, 2014]

STIPULATION REGARDING CONTEMPT ORDER

In response to the Court's order of August 29, 2014, lifting the stay in execution of the July 31, 2014 order, the parties to this proceeding, Microsoft Corporation and the United States of America, hereby jointly stipulate:

1. Microsoft has not fully complied with the Warrant, and Microsoft does not intend to so comply while it in good faith seeks further review of this Court's July 31 decision rejecting Microsoft's challenge to the Warrant.

2. While Microsoft continues to believe that a contempt order is not required to perfect an appeal, it agrees that the entry of an order of contempt would eliminate any jurisdictional issues on appeal. Thus, while reserving its rights to appeal any contempt order and the underlying July 31 ruling, Microsoft concurs with the Government that entry of such

an order will avoid delays and facilitate a prompt appeal in this case.

3. The parties further agree that contempt sanctions need not be imposed at this time. The Government, however, reserves its right to seek sanctions, in addition to the contempt order, in the case of (a) materially changed circumstances in the underlying criminal investigation, or (b) the Second Circuit's issuance of the mandate in the appeal, if this Court's order is affirmed and Microsoft continues not to comply with it.

Accordingly, to facilitate appellate review of this Court's July 31 ruling, the parties jointly request that the Court enter the attached order.

Dated: Sept. 4, 2014
New York, New York

Respectfully submitted,

PREET BHARARA
United States Attorney

By: : /s/ JUSTIN ANDERSON
JUSTIN ANDERSON
SERRIN TURNER
Assistant United States Attorneys
(212) 637-1035 / -1946

Counsel for the United States of America

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Action Nos. 13-MAG-2814, M9-150

IN THE MATTER OF THE SEARCH OF THE PREMISES KNOWN AND DESCRIBED AS THE EMAIL ACCOUNT [REDACTED]@MSN.COM, WHICH IS CONTROLLED BY MICROSOFT CORPORATION

[Filed: Apr. 25, 2014]

DECLARATION OF [REDACTED]

I, [REDACTED] declare as follows:

1. I am a Lead Program Manager for Microsoft Corporation. I have worked for Microsoft since 2002. I have a B.S. from Stanford University and have worked in Hotmail/Outlook.com as an infrastructure Program Manager/Lead Program Manager during my tenure at Microsoft.

2. In my current position, I am responsible for managing the storage "backend" for Outlook.com, which is the current Internet domain name for Microsoft's web-based customer email service. This means that I manage the software and hardware that stores Outlook.com users' emails in Microsoft datacenters so that they can be accessed remotely by users from a variety of mobile and desktop computing devices. I have personal knowledge of the facts stated in this declaration.

3. Microsoft has owned and operated free, web-based email since at least 1997, and this service has operated at various times under different domain names, including Hotmail.com, MSN.com, and Outlook.com. Outlook.com was created in 2013. Users with Outlook.com accounts log on to the service by navigating to the "Outlook.com" web address and by providing their usernames and passwords. Users can also access Outlook.com through their mobile devices. Once they have logged in, users are able to send and receive email messages and store messages in personalized folders.

4. Email messages contain two basic categories of information. First, messages contain content information: the body of an email and its subject line. Second, messages contain non-content information about the email message, such as its sender, the address of its recipient, and the date and time of transmission.

5. Messages sent and received by users of Microsoft's web-based email service are stored in Microsoft datacenters. Microsoft, through its wholly-owned Irish subsidiary, Microsoft Ireland Operations Limited, leases and operates a datacenter in Dublin, Ireland. Starting in September 2010, Microsoft began storing data for certain web-based email accounts in the Dublin datacenter. **[REDACTED]** Microsoft stores email account data in the Dublin datacenter depending on information provided by the user during account registration process. Specifically, when a user first activates a new account, he or she is asked a series of questions, including "Where are you from?" In response to this question, a user must choose a country from a drop-down menu, and

each country is assigned a unique country code. Accounts associated with certain country codes are hosted from the Dublin datacenter [REDACTED]

6. Microsoft decides where to store email account data in part to reduce "network latency." Network latency is the principle of network architecture that the greater the geographic distance between a user and the datacenter where the user's data is stored, the slower the service. The advantage of storing email account data in Dublin is that it allows Microsoft to enhance network efficiency for its users.

7. [REDACTED] Several times each day, Microsoft's backend software runs an automatic scan to determine whether newly-created accounts should be migrated to the Dublin datacenter based on their country code. Once an account is migrated to the Dublin datacenter, all content and non-content information associated with the account in the United States is marked for deletion and is subsequently deleted from Microsoft's U.S.-based servers.

8. For each web-based email account, several copies of the email content and non-content information are created for purposes of redundancy, and the redundant copies are updated on a continuous basis. For accounts stored in Dublin, none of the redundant copies of data are stored in the United States.

9. With the three exceptions discussed below, web-based email user data stored in Dublin is not stored in the United States. Thus, with these three exceptions, if Microsoft were to receive a legal demand from the

government for user data stored in Dublin, the only way to access that data would be from the Dublin datacenter.

10. The three exceptions referred to above are: (1) for testing and quality control purposes, Microsoft operates a "data warehouse" in the United States that contains certain non-content information about web-based email accounts, including accounts stored in Dublin; (2) for certain web-based email accounts, including accounts hosted from Dublin, users' online "address book" information is stored in Micrsoft's "address book clearing house" ("ABCH"), another centralized database stored on servers in the United States; and (3) Microsoft maintains in the United States a database of basic non-content information about web-based email user accounts, such as the name and country provided during registration.

11. Subject to these three exceptions, all account information associated with Microsoft web-based email accounts hosted in Dublin is stored exclusively in Dublin and can be accessed only from the Dublin datacenter.

* * *

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Dated: [12/17/13]
[REDACTED]

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Action Nos. 13-MAG-2814, M9-150

IN THE MATTER OF THE SEARCH OF THE PREMISES KNOWN AND DESCRIBED AS THE EMAIL ACCOUNT [REDACTED]@MSN.COM, WHICH IS CONTROLLED BY MICROSOFT CORPORATION

[Filed: Apr. 25, 2014]

DECLARATION OF [REDACTED]

I, **[REDACTED]** declare as follows:

1. I am a Program Manager for Microsoft Corporation. I have worked for Microsoft since 2009. I attended Carnegie Mellon from 2005-2009 and received a BS in computer science. I have worked on Microsoft's web-based email services since 2009.

2. In my current position, I am responsible for the tools used to respond to requests by law enforcement agencies for information stored by Microsoft's web-based email service, which currently is called Outlook.com. I have personal knowledge of the facts stated in this declaration.

3. When Microsoft receives a search warrant for stored electronic information, the Global Criminal Compli-

ance ("GCC") team is responsible for handling the response. The GCC team works from offices in the United States (in California and Washington).

4. The GCC team uses a database management program [REDACTED] tool to collect the data sought by search warrants. The [REDACTED] tool [REDACTED] is accessed via a web user interface.

5. When collecting email account data sought by a search warrant, a GCC team member first determines the location of the Microsoft server on which the data is stored. To do this, the GCC team member logs into [REDACTED] and enters certain identifying information about the user account for which data is sought. The [REDACTED] tool then locates the account and determines where data for the account is stored.

6. Once a GCC team member has located the data, the team member may then [REDACTED] collect the requested information from the server on which the user's account is stored. [REDACTED]

7. I have reviewed the warrant issued to Microsoft on December 4, 2013, by the United States District Court for the Southern District of New York (the "Warrant"). A true and accurate copy of the Warrant is attached to this declaration as **Exhibit 1**. I have entered the account information from the Warrant [REDACTED] determined the location of the user data, and ascertained that the data for the targeted account is stored on Microsoft's servers in Microsoft's datacenter in Dublin, Ireland.

8. I also attach to this declaration as **Exhibit 2** a true and accurate copy of a custodian of records form

prepared by GCC, certifying that any information associated with the targeted user account that may be stored in the United States has been produced to the Government.

* * *

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Dated: [12/17/13] Signed: **[REDACTED]**

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

REDACTED
Action Nos. 13-MAG-2814, M9-150

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

[Filed: June 6, 2014]

DECLARATION OF [REDACTED]

I, **[REDACTED]** declare as follows:

1. I am a Senior Compliance Manager for Microsoft Corporation in Ireland. I have worked for Microsoft since June 2010. In my current position, I am responsible for responding to legal orders for customer data that Microsoft receives from Irish law enforcement. I have personal knowledge of the facts stated in this declaration.

2. When Irish law enforcement authorities seek the content of customer emails stored on Outlook.com, Microsoft's free web-based email service, they generally follow a four-step process. By the "content of customer emails," I mean the body of the email and its subject line as opposed to metadata about the email, such as the date and time it was sent.

3. First, Irish law enforcement authorities submit a legal request addressed to Microsoft Corporation in Redmond, WA, USA, for basic subscriber information about a specified Outlook.com account. These requests are submitted under Section 8(b) of the Data Protection Act of 1998, or under specific legislation pertaining to the investigation, such as the Child Trafficking and Pornography Act of 1998. Microsoft complies with valid requests from Irish law enforcement and produces this information.

4. Second, if Irish law enforcement wishes to obtain additional information about the account in question, they ordinarily will follow up with an additional request inquiring as to the location of the data—*e.g.*, whether it is stored in our Dublin datacenter or elsewhere.

5. Third, if the email content data for the specified account is stored in the Dublin datacenter, Irish law enforcement will then obtain a warrant or court order for the data, as required under Irish law. Microsoft will not produce email content to Irish law enforcement that is stored outside of Ireland. For example, when Irish law enforcement has sought to obtain Microsoft user email content data stored in Microsoft datacenters located in the United States, I have referred them to the procedures available to them under United States-Ireland Mutual Legal Assistance Treaty.

6. Fourth, Irish law enforcement then arranges to serve me personally with a warrant or court order for the email content, which is generally directed both to Microsoft Corporation (in the United States) and to its Irish subsidiary. Under Irish law, I have seven days after receipt of the court order or warrant to produce

the required customer content. During my tenure, we have always met the deadline for producing the requested data.

* * *

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Dated: [6/3/2014]

Signed: [REDACTED]

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

REDACTED

Action Nos. 13-MAG-2814, M9-150

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

[Filed: June 5, 2014]

DECLARATION OF RAJESH JHA

I, Rajesh Jha, declare as follows:

1. I am a Corporate Vice President at Microsoft Corporation. I have worked for Microsoft since 1990. I began as a software design engineer. I have worked on various products and services throughout my Microsoft career. In my current position, I am responsible for leading Microsoft's Outlook/Office 365 Shared organization within the Application & Services Group. In this capacity I lead development and service engineering for Microsoft's Office 365 enterprise and Outlook.com consumer services, among several other engineering responsibilities. Outlook.com is the successor to Hotmail, and to MSN email services (i.e. the service at issue in this case.) I also lead the Application & Services Group's engineering teams in Norway and China. I have a master's degree in computer science from the University of Massachusetts, Amherst and a bachelor's

degree in computer science from Indian Institute of Technology, Madras (Chennai). I have personal knowledge of the facts stated in this declaration.

2. Cloud computing is the use of connected computers and network resources to enable providers such as Microsoft, Google and Amazon to deliver computing resources to users as a service over the Internet. These services made available to the general public (or "public cloud services") can be operated at tremendous scale and provide users with the resources to run applications, store data, or perform other computing tasks. Historically, businesses, governments and educational institutions were required to make substantial investments in their own computing hardware, software and infrastructure in order to provide their users with such computing capabilities. With the development, availability and adoption of public cloud services, the need for such investment is increasingly becoming unnecessary. Cloud services also ensure that customers always have the most up-to-date computing resources available.

3. This shift in computing has been transformative. It provides tremendous efficiencies to traditional computing-intensive enterprises by enabling them to invest resources in core purposes as opposed to IT infrastructure. It also unleashes incredible productivity opportunities for enterprises that previously could not afford, or were otherwise unable to make, the investments in information technology that have generally been required. It has also provided tremendous value to consumers—who are able to use cloud computing to

obtain free or inexpensive use of vast computer resources to access services, communicate with one another, and store their personal data.

4. Microsoft offers several enterprise public cloud services used by businesses, governments and educational institutions worldwide. These include, but are not limited to, Office 365 (a suite of software applications for commercial productivity services, including email and word processing), Microsoft Azure (platform and infrastructure resources to build, deploy and manage applications and services globally), and CRM Online (sales productivity and resource management services). Microsoft also offers consumer cloud services such as Outlook.com, which provides email and instant message communications to millions of users throughout the world.

5. Microsoft's enterprise cloud service offerings are made available in 100+ countries through a regionally segmented public cloud. This means that Microsoft's public cloud is segmented into regions, and most customer data (e.g. email, calendar entries, and documents) is generally contained entirely within one or more data centers in the region in which the customer is located. This is the most scalable, reliable and cost effective approach. We believe other large enterprise cloud vendors have taken a similar approach. Microsoft stores data for its major enterprise public cloud services in data centers throughout the world in North America, Latin America, Europe and Asia. Some of the countries in which we currently host customer data include the United States, Ireland, the Netherlands, Japan and Brazil. This regional implementation is driven

by engineering and business capabilities and constraints, as well as key imperatives such as optimizing for performance and communications latency minimization to deliver outstanding user experiences. **[REDACTED]**

6. Microsoft's global datacenter footprint for its enterprise and consumer cloud services is one of the largest in the world, and growing rapidly to accommodate what we expect will be growing customer demand for our cloud services. We currently manage over one million server computers in our datacenters worldwide, in over 100 discrete leased and owned datacenter facilities spread over 40 countries. Further, it is conceivable that to accommodate the broader shift to cloud computing, each of these numbers could double over the next several years. These facilities host more than 200 online services, used by over 1 billion customers and over 20 million businesses worldwide.

7. The transition to the cloud by consumers and enterprises worldwide is accelerating at a rapid pace. Consumers increasingly store pictures, video, communications and private documents in the cloud, and access cloud computing services as part of their everyday life. Businesses, governments and educational institutions are increasingly taking critical dependencies on public cloud computing solutions, and shifting their information technology investments to such offerings. Based on industry and analyst data, we believe public cloud services will grow significantly over the coming years, and at a much higher rate than the information technology industry as a whole. In 2013, International Data Corporation (IDC) forecasted worldwide spending on public cloud services to reach almost $59 billion in

2014, with slightly less than half from outside of the United States. IDC also forecasted that information technology industry spend on public cloud services outside of the United States will be approximately $60 billion in 2017. Further, growth of cloud adoption outside the United States is expected to surpass domestic growth, and public cloud spending outside of the United States will account for more than 55% of worldwide public cloud spending by 2017. This tremendous growth is fueled by the efficiencies and economic benefit that cloud computing promises. Relative to traditional information technology spend by enterprises, cloud services are estimated to save customers as much as 30% to 40% per year.

8. In the year since disclosures by Edward Snowden regarding surveillance practices by the United States Government, Microsoft partners and enterprise customers around the world and across all sectors have raised concerns about the United States Government's access to customer data stored by Microsoft. These concerns relate not only to the actual and perceived practices of the National Security Agency that have been described following the disclosures by Edward Snowden, but there is also clearly a heightened concern, as a general matter, about United States government access to customer data stored in data centers located outside of the United States that are operated by United States cloud service providers. The notion, of United States government access to such data—particularly without notice to the customer—is extremely troubling to our partners and enterprise customers located outside of the United States.

9. These concerns of our partners and customers located outside of the United States have manifested themselves in a number of ways. The concerns are often a substantive topic of discussion in briefings or contract negotiations, and they create friction in the sales process and have a chilling effect on the business. Some customers have delayed a transition to cloud services until the environment around these issues is more settled. Other customers ave chosen to not purchase public cloud services from Microsoft at all, and have instead opted for a non-cloud solution. Both of the foregoing result in customers maintaining the status quo of an aging, uncompetitive, less secure and more expensive information technology infrastructure. Customers have also acquired cloud services from a provider based outside of the United States that is perceived as not being subject to United States jurisdiction.

10. Some of these customers referred specifically to the decision in this case by Magistrate Judge Francis as a basis for concern about the United States Government's access to customer data. Although this case involves consumer cloud services, namely Outlook.com email services, many of our partners and enterprise customers (e.g. business and foreign government enterprises) see the U.S, government's unilateral approach to obtaining private data in this case as a threat to the privacy and protection of enterprise data as well. This concern is greatly reduced when the U.S. government is perceived to be acting in cooperation with their counterparts in other governments (thereby ensuring local enterprises that they remain entitled to the privacy and procedural protections of their own governments).

11. This perception of unilateral United States Government access to customer data situated in data centers outside of the United States will in my belief have a substantive negative impact on our public cloud business model. Transition to the public cloud, whether by enterprises or consumers, requires trust in the cloud service provider to deliver a secure and reliable cloud service. An absolute imperative is that the cloud service provider protect the integrity and privacy of its customers' data. Microsoft has made significant investments in the security and reliability of its cloud services to protect customer data. Microsoft has also made significant capital investments in the establishment of data centers situated regionally throughout the world to address customer expectations relative to the location of data storage. Our customers around the world, through their decision to move to our cloud services, have demonstrated that they trust Microsoft and have confidence in the technical and operational safeguards we deploy to protect their data. However, in the wake of the Edward Snowden disclosures and the decision in this case by Magistrate Judge Francis, enterprises any consumers have also clearly indicated that the perception of unilateral government access to their data is undermining that trust and confidence.

12. Ultimately, these concerns will impact the ability of Microsoft and other United States cloud providers to remain competitive in the global marketplace. To the extent foreign enterprises and consumers perceive that their data entrusted to United States cloud service providers, even when that data resides outside of the United States, is subject to unilateral access by the

United States government, there will be increasing demand for national public clouds operated by cloud service providers perceived as not subject to United States Government jurisdiction. Microsoft and other U.S. companies will lose market share, and as a result, the compelling opportunity that cloud computing offers to our customers through cost savings, productivity gains, and access to the latest information technologies will not be fully realized.

* * *

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Dated: [June 5, 2014]

Signed: /s/ RAJESH JHA
RAJESH JHA

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Action Nos. 13-MAG-2814, M9-150

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

[Filed: June 6, 2014]

DECLARATION OF MICHAEL MCDOWELL

I, **MICHAEL MCDOWELL**, declare as follows:

1. I am a Senior Counsel at the Bar of Ireland, having been called to the Bar in 1974 and to the Inner Bar in 1987. I was Attorney General of Ireland from 1999 to 2002, Minister of Justice Equality and Law Reform from 2002 to 2007, and Deputy Prime Minister from 2006 to 2007. I left govermment service in 2007, and I am now in practice as a Senior Counsel in the Irish High and Supreme Courts. I have been engaged by Microsoft as an independent expert to opine on the issues raised in this case.

2. As Attorney General of Ireland, I was legal advisor to the Irish Government during the negotiation and implementation of the Mutual Legal Assistance Treaty Between the United States and Ireland, signed January 18, 2001 (the "U.S.-Ireland MLAT"). In 2003, the European Union and the United States entered a separate agreement on mutual assistance, which was

subsequently applied in relation the U.S.-Ireland MLAT. The MLA treaties between Ireland and the United States were intended by the treaty signatories to serve as the means for law enforcement authorities in the respective countries to obtain evidence located in the other treaty party.

3. In 2008, Ireland enacted the Criminal Justice (Mutual Assistance) Act, 2008 to provide for procedures for responding effectively to requests made under these international agreements (the "2008 Act"). Pursuant to these procedures qualified U.S. authorities are able to seek the assistance of the Irish state in obtaining evidence located in Ireland that may be relevant to criminal investigations or proceedings in the United States.

4. Requests for assistance are evaluated by Ireland's Central Authority for Mutual Assistance (the "Central Authority"), which is part of the Department of Justice and Equality. Provided that the assistance requested by the United States would comply with the standards established in the 2008 Act—*e.g.*, compliance would not prejudice Irish security or sovereignty—the Central Authority will execute the request. Refusal by Ireland to execute a proper request duly made for assistance from U.S. authorities is very uncommon.

5. To fulfill a request for assistance, the Central Authority, forwards the request to An Garda Síochána Ireland's national police service. Where the information sought is email content. An Garda Síochána apply on an ex parte basis for a search warrant or order from an Irish district court judge.

6. If the application submitted to the court satisfies the legal standards set out in the 2008 Act, the judge then forthwith issues a warrant authorising An Garda Síochána to conduct a search of the places or persons identified in the application, or an order requiring persons (including webmail service providers) to produce the requested materials. The police may then execute the warrant or in the case of an order, serve it upon the appropriate recipient.

7. Webmail service providers in Ireland must comply with any warrant or order issued by a district court judge. To obstruct the Garda Síochána's execution of such process is a criminal offense that carries punishment of six months' imprisonment or a €2500 fine.

8. The 2008 Act procedures are a highly effective means of realizing the MLA treaties' objectives. Ireland rarely refuses requests for information made under the treaties, as noted above and the current MLAT procedures for fulfilling these requests are efficient and well-functioning.

9. In the present case, I understand that U.S. law enforcement seeks email content stored on Microsoft's servers in Dublin, Ireland. The aforementioned treaties and procedures were designed to apply under precisely these circumstances. The U.S government should therefore obtain the evidence it seeks through the MLA treaties.

10. Ireland's Data Protection Acts, 1998 to 2003, highlight its sovereign interest in guarding against the exercise of foreign law enforcement activities within its borders by any means other than the applicable MLA

treaties. As a sovereign state and member state of the European Union, Ireland's data protection law, in accordance with EU Directives and the Council of Europe Convention on Data Protection, requires Ireland to protect the rights of data subjects in relation to data located in the jurisdiction of Ireland. Absent certain particular exceptions, disclosure to a third party of such data (*i.e.*, data that is stored and processed in Ireland) is only lawful pursuant to orders made by the Irish courts. And in such cases, any disclosure to a third party on the grounds of "legal obligation" or that it is "necessary for the administration of justice" is only lawful where such disclosure is required or mandated by reference to Irish law and subject to the jurisdiction and control of the Irish courts.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on 5 June 2014.

Signed: /s/ MICHAEL MCDOWELL
MICHAEL MCDOWELL

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Case Nos. 13-MAG-2814; M9-150

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

[Filed: June 6, 2014]

DECLARATION OF CLAIRE CATALANO

CLAIRE CATALANO, pursuant to 28 U.S.C. § 1746, declares as follows under penalties of perjury:

1. I am an attorney duly admitted to practice before this Court, and an associate of the firm Covington & Burling LLP, counsel for Microsoft Corporation.

2. I submit this declaration in support of the above-referenced motion.

3. I attach as Exhibit 1 a true and correct copy of an Email from Christopher B. Harwood, Assistant United States Attorney, United States Attorney's Office for the Southern District of New York, to Nathan Wessler, American Civil Liberties Union, dated April 19, 2013, *available at* http://www.aclu.org/files/pdfs/email-content-foia/EOUSA%20docs/EOUSA%20response%20email%204.19.13.pdf.

4. I attach as Exhibit 2 a true and correct copy of an article titled "How Brazil and the EU Are Breaking

the Internet," published by Forbes on May 19, 2014, *available at* http://www.forbes.com/sites/elisugarman/2014/05/19/how-brazil-and-the-eu-are-breaking-the-internet/.

5. I attach as Exhibit 3 a true and correct copy of a Letter from Sophie in't Veld, Member of the European Parliament, to Viviane Reding, Vice-President of the European Commission, dated April 28, 2014, *available at* http://www.statewatch.org/news/2014/may/ep-letter-to-Vice-President-Reding-on-extraterritorial-jurisdiction-US-Stored-Communications-Actunsigned.pdf.

6. I attach as Exhibit 4 a true and correct copy of an article titled "Microsoft 'must release' data held on Dublin server," published by the British Broadcasting Corporation on April 29, 2014, *available at* http://www.bbc.com/news/technology-27191500.

7. I attach as Exhibit 5 a true and correct copy of a Memorandum from the European Commission titled "Restoring Trust in EU-US data flows—Frequently Asked Questions," dated November 27, 2013, *available at* http://europa.eu/rapid/press-release_MEM0-13-1059_en.htm.

Dated: June 6, 2014
New York, NY

/s/ CLAIRE CATALANO
CLARE CATALANO, ESQ.

EXHIBIT 1

Nathan Wessler

From: Harwood, Christopher (USANYS) <Christopher.Harwood@usdoj.gov>
Sent: Friday, Apr. 19, 2013 4:59 PM
To: Nathan Wessler
Subject: ACLU v. DOJ, No. 12-4677

Dear Nate,

Pursuant to paragraphs 1 and 2 of the parties' stipulation dated March 22, 2013, EOUSA was required to ask the current Criminal Chiefs in the United States Attorneys' Offices for the Southern District of New York, the Eastern District of New York, the Northern District of Illinois, the Northern District of California, the Eastern District of Michigan, and the Southern District of Florida whether, since *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), their respective Offices have ever authorized a request to a court for access to the contents of a person's private electronic communications for law enforcement purposes without a warrant or on a standard less than probable cause. By April 19, 2013, EOUSA was required to inform ACLU, in writing, how each of the relevant Criminal Chiefs responded.

I write on behalf of EOUSA to report that each of the Criminal Chiefs responded, "no."

Please let me know if you have any questions.

Chris

Christopher B. Harwood
Assistant United States Attorney
Sourthern District of New York
86 Chambers Street
New York, NY 10007
Telephone: (212) 637-2728
Facsimile: (212) 637-2786
Email: christopher.harwood@usdoj.gov

EXHIBIT 3

Brussels, 28 Apr. 2014

Dear Vice-President Reding,

On Friday 25 April 2014, a US federal judge ruled that search warrants issued by US law enforcement authorities on the basis of the US Stored Communications Act extend to overseas email accounts.[1] This ruling again confirms that US authorities are able to obtain personal data of European citizens stored on EU territory. Does the Commission that companies complying with such a warrant of a third country would be in breach of European and national data protection law?

Furthermore, how does the Commission assess this ruling of the US federal judge, and the impact of the US extraterritorial jurisdiction on the communications of European citizens? How does the Commission assess the impact of US extraterritorial jurisdiction on transatlantic agreements such as mutual legal assistance treaties, the EU US Passenger Name Record Agreement, the EU US TFTP Agreement, the Safe Harbour programme and the EU US umbrella agreement which is currently being negotiated?

Is the Commission aware of any other third country, for instance the Russia, exerting extraterritorial jurisdiction over personal data stored on European territory? How would the Commission respond to a breach in the protection of personal data on European soil through the extraterritorial jurisdiction of any other third country?

---

[1] Reuters, 25 April 2014, *U.S. judge rules search warrants extend to overseas email accounts*, link: http://www.reuters.com/article/2014/04/25/us-usa-tech-warrants-idUSBREA3024P20140425

Has the Commission asked the US authorities for clarification? If not, why not? How is the Commission going to assure the European citizens that their personal data are protected against extraterritorial jurisdiction of third countries?

I urgently request the Commission to take serious steps in order to avoid any such violation of the European citizens' fundamental rights.

Kind regards,

Sophie in't Veld

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Case Nos. 13-MAG-2814; M9-150

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

[Filed: July 24, 2014]

SUPPLEMENTAL DECLARATION OF CLAIRE CATALANO

CLAIRE CATALANO, pursuant to 28 U.S.C. § 1746, declares as follows under penalties of perjury:

1. I am attorney duly admitted to practice before this Court, and an associate of the firm Covington & Burling LLP, counsel for Microsoft Corporation.

2. I submit this supplemental declaration in support of the above-referenced motion

3. I attach as Exhibit 1 a true and correct copy of a letter from Viviane Reding, Vice-President of the European Commission Justice, Fundamental Rights and Citizenship, to Ms. in't Veld, dated June 24, 2014.

4. I attach as Exhibit 2 a true and correct copy of a certified translation of an article titled "US Wants to Rule over All Servers Globally," written by Christian Kahle on July 24, 2014, *available at* http://winfuture.de/news,82668.html.

5. I attach as Exhibit 3 a true and correct copy of a certified translation of an article titled "US Government to Microsoft: 'Data stored online are not protected under the Fourth Amendment'," written by Franceso Lanza on July 15, 2014, *available at* http://www.downloadblog.it/post/112383/il-governo-usa-contro-microsoft-i-dati-conservati-online-non-sono-protetti-dal-4-emendamento.

6. I attach as Exhibit 4 a true and correct copy of a certified translation of an article titled "US Government: Microsoft Servers Subject to US Laws, Irrespective of Country," published by Inside Channels on July 15, 2014, *available at* http://www.inside-channels.ch/articles/37013.

7. I attach as Exhibit 5 a true and correct copy of a certified translation of an article titled "US Government Accessing Data on Foreign Servers," published by Neue Zürcher Zeitung on July 15, 2014, *available at* http://www.nzz.ch/mehr/digital/usa-microsoft-irland-1.18344021.

8. I attach as Exhibit 6 a true and correct copy of a certified translation of an article titled "Obama also demands access to data stored outside US," published by Data News in Dutch on July 15, 2014, *available at* http://datanews.knack.be/ict/nieuws/obama-eist-ook-toegang-tot-data-opgeslagen-buiten-de-vs/article-4000692430542.htm.

9. I attach as Exhibit 7 a true and correct copy of a certified translation of an article titled "Obama Also Demands Access to Data Stored Outside of the USA," published by Data News in French on July 15, 2014,

available at http://datanews.levif.be/ict/actualite/obama-reclame-aussi-l-acces-aux-donnees-stockees-en-dehors-des-usa/article-4000692595991.htm.

10. I attach as Exhibit 8 a true and correct copy of a certified translation of an article titled "US Government Requests Access to Data Held Abroad," published by Der Standard on July 15, 2014, *available at* http://derstandard.at/2000003099483/US-Regierung-fordert-Zugriff-auf-Daten-im-Ausland.

11. I attach as Exhibit 9 a true and correct copy of a certified translation of an article titled "US Government: Access to Foreign Servers is Lawful," published by Neue Osnabrücker Zeitung on July 15, 2014, *available at* http://www.noz.de/deutschland-welt/gut-zu-wissen/artikel/490495/us-regierung-zugriff-auf-server-im-ausland-ist-rechtens.

12. I attach as Exhibit 10 a true and correct copy of a certified translation of an article titled "US Government Requests Access to Data in EU Processing Centers," published by Heise Online on July 15, 2014, *available at* http://www.heise.de/newsticker/meldung/US-Regierung-fordert-Zugriff-auf-Daten-in-EU-Rechenzentren-2260639.html.

13. I attach as Exhibit 11 a true and correct copy of a certified translation of an article titled "US Also Wants Data from Foreign Servers," published by Future Zone on July 15, 2014, *available at* http://futurezone.at/netzpolitik/usa-wollen-auch-daten-von-auswaertigen-servern/75.024.634.

14. I attach as Exhibit 12 a true and correct copy of an article titled "EU slams US over Microsoft privacy

case," published by the Financial Times on June 30, 2014, *available at* http://www.ft.com/cms/s/0/1bfa7e90-ff6e-11e3-9a4a-00144feab7de.html.

15. I attach as Exhibit 13 a true and correct copy of an article titled "High Court refers Facebook privacy case to Europe," published by the Irish Times on June 19, 2014, *available at* http://www.irishtimes.com/business/sectors/technology/high-court-refers-facebook-privacy-case-to-europe-1.1836657.

16. I attach as Exhibit 14 a true and correct copy of the Irish High Court's decision in *Maximillian Schrems v. Data Protection Commissioner*, dated June 18, 2014.

17. I attach as Exhibit 15 a true and correct copy of the United Kingdom's Data Retention and Investigatory Powers Act 2014, *available at* http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf.

Dated: July 24, 2014
New York, New York

/s/ CLAIRE CATALANO
CLARE CATALANO, ESQ.

EXHIBIT 1

Viviane REDING
Vice-President of the European Commission
Justice, Fundamental Rights and Citizenship

Rue de la Loi, 200
B-1049 Brussels
T. +32 2 298 16 00

Brussels, 24 June 2014

Dear Ms in't Veld,

Thank you for your letter of 13 May concerning the Court of Justice ruling in the Google Spain case.

In its ruling the Court said, in relation to the territoriality of EU rules, that even if the physical server of a company processing data is located outside Europe, EU rules apply to search engine operators if they have a branch or a subsidiary in a Member State.

The Commission has welcomed the Court of Justice's decision. In the global world of digital services, the fundamental rights of EU citizens would be nothing more than empty shells if EU data protection rules were not to apply to non-EU companies. That is why the proposed data protection Regulation, for the first time, leaves no legal doubt that no matter where the physical

server of a company processing data is located, non-EU companies, when offering services to EU consumers, must comply with EU data protection law (this is made explicit in Article 3 of the proposed data protection Regulation).

I am grateful for your support and that of fellow Members for this principle in the Parliament's report on the Commission's proposal. Furthermore, I am pleased that Ministers have reached agreement on this principle at their meeting in Luxembourg on 5-6 June 2014, namely that EU rules should apply to all companies, even those not established in the EU (territorial scope), whenever they handle personal data of individuals in the EU. Ministers have also confirmed a partial general approach on the rules governing transfers of personal data outside the EU, which will ensure that individual rights are protected and that transfers will only be allowed where the conditions of the Regulation for a transfer to third countries are met. This may, inter alia, be the case where the disclosure is necessary for an important ground of public interest recognised in the Union law or in a Member State law to which the controller is subject.

Ms Sophie in't Veld
Member of the European Parliament

In your letter you also refer to the Microsoft case, which concerns a request by the United States government to personal data processed by US companies outside the US, e.g. in the EU. The effect of the US District Court order is that it bypasses existing formal procedures that are agreed between the EU and the US, such as the Mutual Legal Assistance Agreement, that manage foreign

government requests for access to information and ensure certain safeguards in terms of data protection. The Commission's concern is that the extraterritorial application of foreign laws (and orders to companies based thereon) may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union. In addition, companies bound by EU data protection law who receive such a court order are caught in the middle of such situations where there is, as you say in your letter, a conflict of laws.

The Commission has raised this issue with the US government on a number of occasions. The Commission remains of the view that where governments need to request personal data held by private companies and located in the EU, requests should not be directly addressed to the companies but should proceed via agreed formal channels of co-operation between public authorities, such as the mutual legal assistance agreements or sectorial EU-US agreements authorising such transfers. In the context of the negotitaions on the umbrella agreement on data protection in the area of law enforcement and judicial cooperation, the Commission has asked the US to undertake commitments in that regard, in order to avoid these potential conflicts of laws. In parallel, the EU insitutions should continue working towards the swift adoption of the EU data protection reform, in order to ensure that personal data is effectively and comprehensively protected.

/s/ [ILLEGIBLE]

EXHIBIT 2

[advertisements]

US Wants to Rule over All Servers Globally

In the USA, a discussion has broken out about how far the arm of the US justice department may reach. At least the government is of the opinion that US agencies may access servers anywhere in the world, provided they have the respective court order.

The dispute started following a court order that software company Microsoft should provide criminal investigators in the USA with information stored on a server in Ireland. The court was of the opinion that the company had to obey the request, regardless of where it had actually stored the data, according to Ars Technica.

The US government had also previously clarified its position on the legal situation: data stored on the Internet could not be compared to information stored in another country on a non-digital medium. Since Microsoft has access to the data in question from inside the USA, the request for release had to be granted.

Microsoft of course sees this differently and has appealed to the US Supreme Court. The company lawyers make it clear that a US court has no right to a decision enabling federal agents to enter a data center in Dublin to seize things. In separate statements, other IT and telecommunications companies such as Apple, AT&T, Cisco and Verizon backed up the software company in Redmond.

US economy threatened

In addition to the fundamental legal questions, Microsoft also brought up the current situation in its field, according to which it would be a great setback for the IT industry if the order was upheld. Due to the revelations by Edward Snowden, the trust of Internet users in US providers has already clearly suffered. Should the US government succeed with its position in the current case, this would constitute moving the US IT industry a further step ahead in losing its leading role in the global market one day.

[text at right]
Date: Thursday, 7/25/2014 10:56am
Further Reading: Rights, Politics & EU
Author: Christian Kahle

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257

LanguageWorks

[SEAL OMITTED]

STATE OF NEW YORK

v.

COUNTY OF NEW YORK

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "US-Regierung will Verfügungsmacht über alle Server weltweit" completed on 07/22/2014, originally written in German.

/s/ KEVIN HUDSON
KEVIN HUDSON
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014

/s/ MARCEL HENRIQUE VOTLUCKA
Notary Public

[NOTARY STAMP OMITTED]

EXHIBIT 3

TECHNOLOGY

Homepage > Digital rights

US Government to Microsoft: "Data stored online are not protected under the Fourth Amendment"

Written by: Francesco Lanza—Tuesday, July 15, 2014

The Fourth Amendment to the US Constitution prohibits unreasonable searches and seizures, but the US government doesn't want that right applied to data stored online, especially abroad.

Microsoft tried to shield a user whose data are stored in its storage centers in **Dublin**, seeking to have the **international search warrants** issued by a New York judge declared unconstitutional. The US government was completely against this and reacted aggressively to attempts to rein in its wide-ranging powers of investigation.

In an official statement released yesterday, the government stated that data stored in the cloud are not granted the same type of protection afforded to "physical" information, protected under the **Fourth Amendment to the US Constitution**. In fact, according to the Stored Communications Act, such data have always been much more accessible than normal correspondence and private assets held abroad.

READ ALSO: ProtonMail, the e-mail service the NSA can't penetrate

These days, hackers and scammers who use electronic communication methods both in the United States and abroad in an attempt to get around the law, make this double standard a necessity.

It seems as though the US government is the only party not concerned about the implications of its sprawling control over the entire planet's data, and even **Verizon** has joined forces with **Microsoft** to contend that these arguments are in direct conflict with foreign laws on data protection. **Apple** and **Cisco** have responded similarly, saying that the US government seems fully determined to damage commercial and diplomatic relationships with both allied and non-aligned countries.

INSIGHT: Obama authorizes the use of software vulnerabilities for espionage and investigations

In fact, the White House's legal argument simply adds fuel to the fire of the media disaster known as the **Snowden** affair.

For its part, the Irish government does not seem at all concerned about the long-term damage caused by US legal rulings; on the contrary, it seems more than willing to provide US investigators with the personal data and access to e-mail that they seek. Actually, that shouldn't be too surprising: the case involves international drug trafficking.

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257

[SEAL OMITTED]

LanguageWorks

STATE OF NEW YORK

v.

COUNTY OF NEW YORK

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of Il Governo USA contro Microsoft: 'I dati conservati online non sono protetti dal 4° Emendamento'" completed on 07/22/2014, originally written in Italian.

/s/ KEVIN HUDSON
KEVIN HUDSON
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014

/s/ MARCEL HENRIQUE VOTLUCKA
Notary Public

[NOTARY STAMP OMITTED]

EXHIBIT 4

[advertisement]

Inside-channels.ch

Tuesday, 7/15/2014

US Government: Microsoft Servers Subject to US Laws, Irrespective of Country

An email account is stirring up the world of the Cloud.

In the USA, a dispute between the US Department of Justice and Microsoft has been going on for a long time. While, in concrete terms, this is merely about the content of an email account stored in Ireland, the outcome of this precedent case could strongly impact the future of cloud business across the globe. The question is whether US judges may force domestic companies to release data stored abroad, regardless of where such data are stored and what laws might apply in the respective country.

A US federal judge will have to address the issue soon. In a recent submission to this judge, the Obama government has now confirmed its legal position and explained that, for criminal prosecution purposes, US agencies need to have access to client data of US companies, even if such data were stored abroad. According to this position, an order by a US judge seeing sufficient indication that certain data could contain relevant data would have to force data to be released. The laws and agencies in the respective country would play no role in this. A "detour" via a legal assistance process and/or cooperation with authorities in the respective country would thus become unnecessary.

To search or not to search?

Throughout, the US government is backing up its request by citing the Stored Communications Act of the Reagan era. Microsoft, on the other hand, argues that this law could not apply abroad. In its view, such a request would correspond to a search warrant, and no US court could order US agents to break open a door at the Microsoft processing center in Dublin, for example, in order to seize data. According to Microsoft, Congress explicitly decided in its favor recently.

The US government, however, considers this argument completely irrelevant since the release of data stored online has nothing in common with a physical search.

In its line of argument, Microsoft is supported by other IT giants such as Apple, AT&T, Cisco and Verizon. A lot of money is at stake for American companies. If the US government prevails, foreign clients' confidence in their cloud-based services, already weakened by the Snowden affair, is likely to decline even further. And employees abroad could end up in a legal dilemma if they had to choose whether to comply with US Justice Department orders or local laws. Foreign branches of US companies have so far adamantly emphasized that they would, of course, always do the latter. (hjm)

More on this topic

Microsoft not (yet) providing data to US government US agencies may continue to access cloud data abroad. Obama's expert group defends NSA practices

[article comments]

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257

[SEAL OMITTED]

LanguageWorks

STATE OF NEW YORK

v.

COUNTY OF NEW YORK

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "US-Regierung: Microsoft-Server unterstehen US-Gesetzen, egal in welchem Land" completed on 07/22/2014, originally written in German.

/s/ KEVIN HUDSON
KEVIN HUDSON
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014

/s/ MARCEL HENRIQUE VOTLUCKA
Notary Public

[NOTARY STAMP OMITTED]

EXHIBIT 5

Neue Zürcher Zeitung

Tuesday, July 15, 2014, 2:22pm

Precedent

US Government Accessing Data on Foreign Servers

Henning Steier Tuesday, July 15, 2014, 2:22pm

[image caption: Who may access processing center data globally? (image: Imago/Symbolfoto)

IT giants are not the only ones who are currently paying close attention to whether the largest software producer will prevail in its court case versus the US government. The decision will have far-reaching consequences for companies and users alike.

In the USA, Microsoft is taking legal action against having to provide US agencies with data stored in computer processing centers outside the United States. The line of argument by the American government in this court case, which will continue in late July, has now become public. In essence, it refers to the Stored Communications Act (SCA) of 1986 and assumes that online content is not protected under the Fourth Amendment. This Amendment concerns protection against federal searches and seizures.

At the end of April, a New York court argued that American companies must release data stored on servers abroad if there is a relevant request by a US government agency. Based on a search warrant in a drug smuggling case, Microsoft was asked to release client data stored on a server in Ireland. The company argued that the principle, according to which court-

ordered search warrants are non-applicable abroad, would also have to be transferred to the online world. Judge James Francis however saw it differently and argued in his decision that the resulting burden would be major and criminal investigations would be gravely obstructed if US agencies first had to send requests for legal assistance to foreign governments.

Loss of trust as business risk

Following the Snowden revelations, the largest software producer fears a further reputational loss for US companies and, as a result, an adverse impact on business in the rest of the world. Other large IT companies see it similarly. Verizon assumes that a decision in favor of the government could result in "conflicts with data protection laws in other countries." Apple and Cisco also fear that the technology sector "runs the danger of being sanctioned by foreign governments."

Microsoft opened its processing center in Ireland four years ago. By now, the company is running approximately 100 in 40 countries. In spring, the *Vereinigung der schweizerischen Datenschutzbeauftragten* (Privatim) prevailed against Microsoft Schweiz by convincing the company to alter its contractual conditions as to permit the use of Office 365 in an academic context. To that end, a contract change specifically applying to the Swiss educational sector was developed, ensuring that usage in compliance with data privacy laws is guaranteed. Concretely, this also means: upon request, data may be stored only in Europe. The present court case in the USA should demonstrate how valuable this is.

Follow Digital editor Henning Steier in Social Networks:

You can order the daily Digital newsletter here.

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257

[SEAL OMITTED]

LanguageWorks

STATE OF NEW YORK

v.

COUNTY OF NEW YORK

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "US-Regierung greift nach Daten in ausländischen Rechenzentren" completed on 07/22/2014, originally written in German.

/s/ KEVIN HUDSON
KEVIN HUDSON
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014

/s/ MARCEL HENRIQUE VOTLUCKA
Notary Public

[NOTARY STAMP OMITTED]

EXHIBIT 6

Obama also demands access to data stored outside US

(http://datanews.knack.be/ict/service/contact/author-1194715612360.htm)
Frederik Tibau (http://datanews.knack.be/ict/service/contact/author-1194715612360.htm) July 15, 2014—10:00

The Obama administration is proposing that data stored on the servers of American companies outside the United States must be accessible to judicial authorities.

Technology companies such as Microsoft and Apple are screaming bloody murder and argue that upholding justice stops at the border.

According to the US government, global access to information is necessary to be better able to track scammers, hackers, and drug dealers. Obama & Co. also argue that any company with operations in the United States must comply with the data requirements of that country, even if the data have been stored on the other side of the world.

Tech giants like Microsoft and Apple do not agree on this and argue that confidence in American technology companies will take yet another blow that way, after the Snowden revelations.

And now one judge has subscribed to Obama's position. During a court case just last April involving a Microsoft customer, he put forward the idea that "an entity that is

statutorily obligated to provide access to data must do so regardless of the location of those data."

Microsoft has already brought in a battery of lawyers to file an appeal. A ruling on the case is expected on July 31.

The US government is relying on the **Stored Communications Act (http://cdn.arstechnica.net/wp-content/uploads/2014/07/federalbrief-microsoftcase.pdf)** (SCA) to hit back, a rule that dates from the Reagan era. That rule states, "Overseas records must be disclosed domestically when a valid subpoena, order, or warrant compels their production."

Microsoft will again argue that the US Congress has never given the order to require information from outside the physical borders of the United States. "Furthermore, an American court cannot just require someone to break into the Microsoft's data center in Dublin," Redmond says. "The only thing that the government will achieve that way is American companies losing their leading position in IT."

Industry partners Apple, AT&T, Cisco, and Verizon **argue (http://cdn.arstechnica.net/wp-content/uploads/2014/07/applebriefinremicrosft.pdf)** that a ruling in favor of the administration may cause "dramatic conflicts with foreign laws on data protection."

These companies argue that "there is a very great risk that foreign governments will penalize the tech industry and that it is better to work together with other nations."

[advertisement below]

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257

[SEAL OMITTED]

LanguageWorks

STATE OF NEW YORK

v.

COUNTY OF NEW YORK

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "Obama eist ook toegang tot data opgeslagen buiten de VS" completed on 07/22/2014, originally written in Dutch.

/s/ KEVIN HUDSON
KEVIN HUDSON
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014

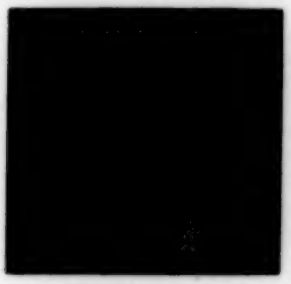
/s/ MARCEL HENRIQUE VOTLUCKA
Notary Public

[NOTARY STAMP OMITTED]

EXHIBIT 7

Obama Also Requires Access to Data Stored Outside of the USA

(http://datanews.levif.be/ict/service/contact/author-1194716134355.htm)
Frederik Tibau (http://datanews.levif.be/ict/service/contact/author-1194716134355.htm) 15/07/2014—14:0



The Obama administration maintains that the data stored on American company servers outside of the United States should be accessible to the American justice system.

Technology companies such as Microsoft and Apple are loudly protesting by arguing that the law stops at the border.

According to the American authorities, worldwide access to information is necessary to better identify smugglers, pirates and other drug dealers. Obama & Co. also maintain that any enterprise doing business in the United States must conform to this country's requirements with regard to data, even if the data are stored on the other side of the planet.

Technology giants such as Microsoft and Apple do not share that opinion; they maintain that confidence in American technology companies will take a direct hit after the Snowden leaks.

A judge has already taken Obama's point of view. During proceedings involving a customer of Microsoft, he already affirmed in April that "an entity that is legally bound to provide access to data must do so regardless of the location of those data."

Microsoft has already resorted to a battery of lawyers to mount an appeal. A final ruling is expected on July 31.

The American authorities are using the Stored Communications Act (SCA) as justification. This is a rule that goes back to the time of Ronald Reagan: "Overseas records must be disclosed domestically when a valid subpoena, order or warrant compels their production," according to this document.

Microsoft, for its part, has asserted that the US Congress has never authorized demands for information from outside the physical boundaries of the United States. "Moreover, an American court cannot thus require access to the Microsoft data center in Dublin," is the response from Redmond. "The only thing that the authorities will gain by acting like this is American enterprises losing their leadership position in the ICT."

Other companies in the sector, such as Apple, AT&T, Cisco and Verizon, maintain that a judgment in favor of the administration would lead to "dramatic conflicts with foreign laws on the subject of data protection."

These businesses say that "there is a very great risk that foreign governments will penalize the technology sector; collaborating with the other nations is therefore the most appropriate thing to do."

[Advertisements unrelated to the text]

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257

[SEAL OMITTED]

LanguageWorks

STATE OF NEW YORK

v.

COUNTY OF NEW YORK

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "Obama réclame aussi l'accès aux données stockées en dehors des USA" completed on 07/22/2014, originally written in French.

/s/ KEVIN HUDSON
KEVIN HUDSON
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014

/s/ MARCEL HENRIQUE VOTLUCKA
Notary Public

[NOTARY STAMP OMITTED]

EXHIBIT 8

derStandard.at > Web > Netzpolitik

US Government Requests Access to Data Held Abroad

July 15, 2014, 4:00pm

Microsoft and other US technology firms asked to release data stored on servers abroad

Microsoft is engaged in a legal dispute with the US Department of Justice. The company has been asked to release data not stored in the USA but on servers in Ireland. Microsoft, as well as other companies, are resisting the request and argue that the enforcement of US American laws would have to be limited to inside its borders.

US government refers to 1986 law

The government, however, refers to the Stored Communications Act of 1986 and argues that the Fourth Amendment on the protection against federal searches and seizures does not cover online content. Microsoft had no right to refer to the principles of extraterritoriality, according to the US government.

Loss of client trust

Microsoft fears that the trial could have far-reaching global consequences. Client confidence has already been low as a result of the exposure of the NSA's surveillance activities, says the company. According to Microsoft, the position of the government in this case would further erode trust, and ultimately also in the leadership of US technology companies in the global market.

Conflict with data privacy laws

Companies such as Apple, AT&T, Cisco and Verizon support Microsoft and foresee "grave conflicts with foreign data protection laws." Constitutional scholars in the USA think that the decision could result in a number of global legal disputes and that this is an important case (wen, derStandard.at, 7/15/2014).

Links

Heise

ArsTechnica

Microsoft

[image caption at left]: The US government wants access to all data of Microsoft, Apple & Co— irrespective of the country where they are stored.

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257

[SEAL OMITTED]

LanguageWorks

STATE OF NEW YORK

v.

COUNTY OF NEW YORK

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "US-Regierung fordent Zugriff auf Daten im Ausland" completed on 07/22/2014, originally written in German.

/s/ KEVIN HUDSON
KEVIN HUDSON
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014

/s/ MARCEL HENRIQUE VOTLUCKA
Notary Public

[NOTARY STAMP OMITTED]

EXHIBIT 9

[advertisement]

Neue Osnabrücker Zeitung

[unrelated webpage buttons]

US Government: Access to Foreign Servers is Lawful

07/15/2014 1:16pm

(image caption: Microsoft fights against US agency access to data stored on foreign servers. Photo shows company headquarters in Redmond. Photo: dpa)

Osnabrück. The US-government is of the opinion that, following approval by the court, its agencies may also access data stored on servers in other countries. Washington has made this clear in a legal dispute with Microsoft. The US government has referred to a law from 1986, as reported by various Internet sources.

In the actual case, the matters concerned an order by an undisclosed US agency directing Microsoft to forward data stored on servers in Ireland to prosecutors in the USA. The case allegedly concerned all received and sent emails, access protocols and all credit card numbers and bank accounts of a certain account, which the agency eyed in the context of drug smuggling investigations.

Microsoft, however, rejected the US agency's request by pointing out that the client data was stored on a company server in Dublin, Ireland, and that US search warrants could not be extended abroad. "A US investigator also cannot simply search a house in a different country. [. . .] We think that this rule should also apply to the online world", the company argued.

The US government has now argued before the court tasked with making a decision during the appeals procedures, that online contents are not protected by the Fourth Amendment (Protection against federal searches and seizures). The English-language Internet site Ars Technica reported on the case by titling it "Obama government holds that the world's servers belong to him."

According to Ars Technica, Microsoft is warning against the global consequences of such a decision. The Internet company is worried about its non-American clients. Just a few months ago, Microsoft announced its intention to protect client data against monitoring by storing them outside the USA.

Apple, AT&T, Cisco and Verizon also spoke up. Apple and Cisco criticized that by releasing such data, US companies would in breach of the (data protection) laws of other countries.

[advertisements]

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257

[SEAL OMITTED]

LanguageWorks

STATE OF NEW YORK

v.

COUNTY OF NEW YORK

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "US-Regierung: Zugriff auf Server im Ausland ist rechtens" completed on 07/22/2014, originally written in German.

/s/ KEVIN HUDSON
KEVIN HUDSON
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014

/s/ MARCEL HENRIQUE VOTLUCKA
Notary Public

[NOTARY STAMP OMITTED]

EXHIBIT 10

[unrelated buttons for webpage]

H Online > News > 2014 > KW 29 > US Government Requests Access to Data in EU Processing Centers

07/15/2014 10:49am

US Government Requests Access to Data in EU Processing Centers

Microsoft battles in court against having to release data in the USA that is not even stored inside the country. The US government has submitted its opinion, making reference to a law from before the Internet era.

The US government is referring to a decades-old law for justifying access to data stored by US services abroad. This bases on **a reply** [http://cdn.arstechnica.net/wp-content/uploads/2014/07/federalbrief-microsoftcase.pdf] to a line of argument by Microsoft that the US company used against the release of emails stored in Ireland, as reported by ***Ars Technica*** [http://arstechnica.com/tech-policy/2014/07/obama-administration-says-the-worlds-servers-are-ours/]. Before the court charged with making a decision on the case, the US government referred to the Stored Communications Act from 1986 and argued that, in its opinion, online contents were not protected by the Fourth Amendment (protection against federal searches and seizures).

This process, with allegedly far-reaching consequences, concerns data stored at a processing center in Ireland. The US government made a request in court for their release in the context of investigations involving drug smugglers. **Microsoft is resisting.**

[photo caption] Can Microsoft protect European data from (legal) access by the US?

[advertisement]

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257

[SEAL OMITTED]

LanguageWorks

STATE OF NEW YORK

v.

COUNTY OF NEW YORK

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "US-Regierung fordert Zugriff auf Daten in EURechenzentren" completed on 07/22/2014, originally written in German.

/s/ KEVIN HUDSON
KEVIN HUDSON
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014

/s/ MARCEL HENRIQUE VOTLUCKA
Notary Public

[NOTARY STAMP OMITTED]

EXHIBIT 11

Data Protection

USA Also Wants Data from Foreign Servers

[image caption: Data are no longer secure anywhere— photo: Benjamin Haas, fotolia]

The US government is of the opinion that any company doing business in the USA must release data upon request, even if those are stored outside the USA.

USA, MICROSOFT, REPORT, DATA PROTECTION

This opinion is currently being put on trial. As reported by Ars Technica, the current case concerns Microsoft having to release emails stored on servers in Dublin, Ireland, to US agencies. In contrast, US companies such as Microsoft and Apple believe that US laws may only apply inside domestic borders. In the first instance back in April, a judge agreed with the government's arguments requesting the release of Microsoft data. The company has appealed and a federal judge will hear the case on July 31st.

In the context of submitting the case, the US government has declared that electronically stored information does not enjoy the same protection as physical documents in the real world. Microsoft, however, is asking the judge to take into account that the trust in US technology firms is already at an all-time low. That, in turn, would jeopardize the dominance of American technology. The US Justice Department claims, however, that global criminal prosecution is necessary since no borders exist online. The disputed emails should help to take out a drug smuggling operation.

(FUTUREZONE) ERSTELLT AM 15.07.2014, 13:24

[Text at left]

Data protection

USA Also Wants Data from Foreign Servers

COMMENTS (0)

MORE ON THIS TOPIC

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257

[SEAL OMITTED]

LanguageWorks

STATE OF NEW YORK

v.

COUNTY OF NEW YORK

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "USA wollen auch Daten von auswärtigen Servern" completed on 07/22/2014, originally written in German.

/s/ KEVIN HUDSON
KEVIN HUDSON
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014

/s/ MARCEL HENRIQUE VOTLUCKA
Notary Public

[NOTARY STAMP OMITTED]

EXHIBIT 12

By continuing to use this site you consent to the use of cookies on your device as described in our **cookie policy** unless you have disabled them. You can change your **cookie settings** at any time but parts of our site will not function correctly without them.

FINANCIAL TIMES

June 30, 2014 11:00 am

EU slams US over Microsoft privacy case

By **Richard Waters** in San Francisco

A US attempt to force Microsoft to hand over emails held on servers in Ireland has drawn a strong rebuke from Brussels in one of the first tests of cross-border privacy raised by cloud computing.

The US demand could contravene international law and should have been handled through the official channels normally used for law enforcement between different regions, according to Viviane Reding, vice-president of the European Commission.

The case comes as US technology is already caught up in a transatlantic privacy dispute over revelations about widespread US internet surveillance.

The demand for information held in a different location from the people it relates to could "hurt the competitiveness of US cloud providers in general", Microsoft warned in a lawsuit challenging the order this year.

The software company added: "Microsoft and US technology companies have faced growing mistrust and concern about their ability to protect the privacy of personal information located outside the US."

A magistrate in New York issued a search warrant late last year requiring Microsoft to give emails belonging to a user of its Outlook email service to US law enforcement agencies. The nature of the case and identity of the suspect were not disclosed.

Microsoft's argument that the US enforcement order amounted to an illegal attempt to enforce a warrant beyond US borders has now won support in Europe, with Ms Reding weighing in on Microsoft's side.

"The commission's concern is that the extraterritorial application of foreign laws [and orders to companies based thereon] may be in breach of international law," she wrote last week in a letter to Sophie in't Veld, a Dutch member of the European Parliament.

She added that the US "may impede the attainment of the protection of individuals guaranteed in the [European] Union".

Rather than trying to force Microsoft to surrender information, she said that the US should have relied on the mutual legal assistance treaties that create a framework for co-operation between law enforcement agencies.

Ms Reding's rebuke came in the same week that the US Supreme Court put new limits on the power of law enforcement agencies to search suspects' mobile devices. The judges ruled unanimously that searches could not be carried out without a warrant.

The mobile phone case marked a historic moment in which the court had recognised the need for greater privacy protection as technology advances, Brad Smith, Microsoft's general counsel, wrote in a blog post on Saturday welcoming the decision. It also marked the first time the Supreme Court has considered privacy issues raised by cloud computing, he said.

RELATED TOPICS United States of America European Commission Internet privacy Data protection

Printed from: http://www.ft.com/cms/s/0/1bfa7e90-ff6e-11e3-9a4a-00144feab7de.html

Print a single copy of this article for personal use. Contact us if you wish to print more to distribute to others.

© THE FINANCIAL TIMES LTD 2014 FT and 'Financial Times' are trademarks of The Financial Times Ltd.

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Action Nos. 13-MAG-2814, M9-150

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

[Filed: July 24, 2014]

DECLARATION OF JOSEPH V. DEMARCO

I, **JOSEPH V. DEMARCO, ESQ.**, pursuant to Title 28, United States Code, Section 1746, declare as follows:

1. I am partner in the law firm of DeVore & DeMarco, LLP, an attorney in good standing to practice law in the State of New York, and am admitted to practice in the United States District Court for the Southern District of New York.

2. At the request of Microsoft Corporation ("Microsoft"), I have prepared this Declaration in connection with the above-captioned litigation. Specifically, in order to aid this Court in a proper resolution of the issues in controversy, Microsoft has requested that I provide my insight and analysis concerning certain practices and procedures related to the preservation of electronic evidence held by electronic communications service providers located outside the United States pending the fulfillment of requests made under Mutual Legal Assistance

treaties ("MLATs") and Letters Rogatory for such evidence by the U.S Department of Justice (the "DOJ").

I. SUMMARY

3. I have reviewed the April 25, 2014, Memorandum and Order of U.S. Magistrate Judge James C. Francis IV (1:13-mj-02814-UA, No. 5), Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion dated June 6, 2014 (1:13-mj-02814-UA, No. 15), the Government's Brief in Support of the Magistrate Judge's Opinion filed on July 9, 2014 (1:13-mj-02814-UA, No. 60), the Council of Europe's Convention on Cybercrime, and the related supporting materials cited herein. Based on my experience and expertise in the field of electronic evidence preservation and collection, as described below, and my review of the aforementioned documents, I am aware that there are several methods of evidence preservation that are used by the DOJ for the purpose of quickly, effectively, and efficiently ensuring that electronic communications and other digital evidence located abroad are preserved pending the execution of formal legal process to obtain such evidence.

II. QUALIFICATIONS

4. I am a founding partner at the law firm of DeVore & DeMarco LLP, where I specialize in counseling clients on complex issues involving information privacy and security, computer intrusions, theft of intellectual property, on-line fraud, and the preservation and collection of digital evidence. From 1997 to 2007, I served as an Assistant United States Attorney for the Southern District of New York, where I founded and headed the Computer Hacking and Intellectual Property

("CHIPs") program, a group of prosecutors dedicated to investigating and prosecuting violations of federal cybercrime laws. From January, 2001, until July, 2001, I served as a visiting Trial Attorney at the Computer Crime and Intellectual Property Section of DOJ in Washington, D.C. ("CCIPS"). At CCIPS, among other things, I was responsible for assisting federal and state prosecutors throughout the United States as well as foreign prosecutors and other law enforcement officials in the preservation and collection of electronic evidence from, among other entities, Internet Service Providers ("ISPs") located inside and outside the United States. In these roles, I personally prepared and facilitated, and was aware of the preparation and facilitation by other law enforcement officials, of emergency requests for electronic evidence, including requests for the preservation and collection of electronic evidence from ISPs and providers of electronic communications services. In addition, I was also responsible for working on CCIPS' policy-related efforts concerning the Council of Europe's (then draft, now final) Convention on Cybercrime (the "Budapest Convention").

5. Since 2007, in my private practice, I have regularly counseled clients on the preservation and collection of electronic evidence in criminal and civil litigations and investigations both domestically and internationally. This has included requests for the emergency preservation of electronic evidence from electronic communications service providers.

6. Since 2002, I have served as an Adjunct Professor at Columbia Law School, where I teach the upper-class Internet and Computer Crimes seminar. I have

spoken throughout the world on a range of cybercrime, digital evidence collection and preservation, cloud computing, e-commerce law, and IP rights enforcement issues. Domestically, I have lectured on the subject of cybercrime and electronic evidence gathering at Harvard Law School, the Practicing Law Institute ("PLI"), the National Advocacy Center, and at the FBI Academy in Quantico, Virginia. Internationally, I have lectured on these subjects to law enforcement officials and lawyers in Europe, Asia, and the Middle East. I am on the Board of Advisors of the *Center for Law and Information Policy* at Fordham University School of Law, and am a member of the Professional Editorial Board of the *Computer Law and Security Review* published by Elsevier. I am also listed in *Chambers USA: America's Leading Lawyers for Business* guide as a leading lawyer nationwide in Privacy and Data Security, and am a *Martindale-Hubbell* AV-rated lawyer in the areas of Computers and Software, Litigation and Internet Law.

7. As a former federal prosecutor and as an attorney in private practice, I have had extensive experience throughout my career with complex issues relating to electronic evidence preservation, collection, and spoliation. For example, as the head of the CHIPs program in the Southern District of New York, I was responsible for supervising and advising Assistant United States Attorneys in the District in a broad variety of criminal cases on how to find and collect electronic evidence—such as the content of e-mails and associated account transmission and subscriber records—from a wide range of sources, both domestically and internationally. In

particular, I regularly reviewed applications for search warrants, court orders, MLAT requests, as well as grand jury subpoenas and administrative subpoenas which called for the production of various forms of electronic evidence. In addition, while at CCIPS, I was responsible for advising foreign law enforcement officials from numerous countries regarding evidence preservation techniques and strategies as they related to U.S. law, as well as with applicable evidence retention, preservation, and access policies and practices of ISPs based in the United States. I provided this advice and assistance in cases involving routine requests for electronic evidence as well as in exigent circumstances where the need for very rapid and efficient action was frequently of paramount importance.

8. In addition to my experience in government, in private practice I have continued to be frequently called upon to provide advice on the preservation and collection of digital evidence. The need for this assistance arises in cases implicating both criminal statues as well as civil causes of action; not infrequently, these requests are either extremely time-sensitive and/or involve high-stakes digital evidence preservation and collection issues. For example, I have provided advice related to the preservation and collection of e-mail communications and other electronic evidence in cases involving extortion, computer hacking, theft of trade secrets, illegal password trafficking, copyright infringement, and harassment and cyber-stalking, among others. I have also frequently been involved in representing clients who have been asked to provide digital evidence and other

assistance to the government in criminal as well as intelligence-related investigations.

9. Based on the above experience, I am familiar with requests to seek evidence preservation and collection from ISPs and similar entities, including through the assistance of foreign law enforcement officials. I am also aware that law enforcement officials outside the United States regularly cooperate with federal and state criminal investigators in the United States to achieve the preservation of electronic evidence for use in investigations and prosecutions. This cooperation both complements and reinforces the MLAT and Letters Rogatory framework and includes (a) direct law-enforcement-to-law-enforcement informal cooperation, (b) a more formal "24/7" network, and (c) the Budapest Convention discussed below.

III. INTERNATIONAL EVIDENCE PRESERVATION IN CRIMINAL INVESTIGATIONS

10. Because of its nature, electronic evidence often can be lost if it is not secured in a timely and efficient manner. Partly as a result of this, in my experience, law enforcement officials in various countries communicate with each other directly in cases involving electronic evidence in order to locate, preserve, and collect such evidence. Based on my experience, such direct cooperation is particularly close between United States and Western European law enforcement officials, as well as between law enforcement officials in the United States and those of English-speaking nations throughout the world.

11. In addition to the direct law-enforcement-to-law-enforcement cooperation noted above, since at least 2001, the DOJ has maintained a "24/7 Network" list of emergency law enforcement contacts committed to assist in the preservation of digital evidence across international borders consistent with national legislation. As its name suggests, this list allows for around-the-clock contact among participants to achieve electronic evidence preservation. The list consists of representatives from dozens of countries around the world.

12. Moreover, on December 29, 2006, the United States ratified the Budapest Convention. Notably, Article 29 of the Convention requires that signatory countries implement laws so that foreign governments can request the preservation of electronic data inside their borders and thus ensure that requested data is "not [] altered, removed or deleted during the period of time required to prepare, transmit and execute a request for mutual assistance to obtain the data."[1] The Convention contemplates that, following preservation pursuant to its mandate, access to data by a foreign nation shall proceed according to established international legal process. Notably, international preservation requests as contemplated by the drafters are quite common.[2]

---

[1] *See* Council of Europe, *Explanatory Report to the Convention on Cybercrime*, available at http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (last visited July 22, 2014).

[2] *See* Cybercrime Convention Committee, *Assessment Report: Implementation of the Preservation Provisions of the Budapest Convention on Cybercrime*, at 17, 49 (January 25, 2013), available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/TCY/TCY2013/TCYreports/TCY_2012_10_Assess_report_v30_public.

Noteworthy too is that the Convention affirms and supports the 24/7 Network discussed above.[3] To be clear, these mechanisms supplement the direct law-enforcement-to-law-enforcement communications which I describe in paragraphs 10 and 11, above.

13. Through law-enforcement-to-law-enforcement cooperation, the 24/7 Network, and the Budapest Convention, U.S. law enforcement officials and their foreign counterparts regularly preserve electronic evidence on behalf of one another, including evidence at ISPs, across international borders.

14. The government states in its brief that MLATs "typically take[] months to process." Gov't Br. 25. Based on my knowledge and experience, there is no "one size fits all" period of time in which MLATs are executed. Rather, the speed at which an MLAT is acted upon is a function of the urgency and priority of that request to law enforcement officials. Many MLATs submitted by United States officials to foreign counterparts are not especially time sensitive or urgent, and part of the period associated with receiving evidence via an MLAT consists of the time that DOJ takes to prepare and transmit the MLAT to foreign counterparts. This involves work at the local United States Attorney's office and/or prosecuting unit at DOJ and, subsequently, at the Office of International Affairs, which is the central office at DOJ to which draft MALTs are regularly forwarded for review, comment, approval, and ultimate

---

pdf (last visited July 22, 2014), (noting that as of 2012 the "U.S. sends and receives hundreds of preservation requests per year").

[3] *Id.* at 4, 12.

transmittal abroad. Importantly, however, in my experience, DOJ officials and relevant foreign executing officials can, and regularly do, move with great alacrity and efficiency in processing, transmitting, and responding to high-priority MLATs.

15. I declare under penalty of perjury that the foregoing is true and correct.

Dated: New York, New York
July 24, 2014

/s/ JOSEPH V. DEMARCO
JOSEPH V. DEMARCO

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Action Nos. 13-MAG-2814, M9-150

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

[Filed: July 23, 2014]

SUPPLEMENTAL DECLARATION OF MICHAEL MCDOWELL

I, **MICHAEL MCDOWELL**, declare as follows:

1. I am a Senior Counsel at the Bar of Ireland, having been called to the Bar in 1974 and to the Inner Bar in 1987. I was Attorney General of Ireland from 1999 to 2002, Minister of Justice, Equality and Law Reform from 2002 to 2007, and Deputy Prime Minister from 2006 to 2007. I left government service in 2007, and I am now in practice as a Senior Counsel in the Irish High and Supreme Courts.

2. I have been engaged by Microsoft as an independent expert to opine on the issues raised in this case. This declaration supplements my declaration of 5 June 2014, and provides additional information in respect of certain statements made by the U.S. Government in its submission of 9 July 2014.

3. Specifically, on page 25 of its submission, the U.S. Government states that an "MLAT request typically takes months to process." This statement is not accurate with respect to MLAT requests processed by the Irish government.

4. The amount of time the Irish government requires to process an MLAT request (*i.e.*, the time from when the request is made until the evidence is received by the foreign MLAT party) depends upon the type and urgency of the request. Some requests, such as a request for a deposition, can take months from start to finish. Other requests, such as requests for digital evidence, are generally fulfilled within a matter of weeks. Furthermore, if a request is urgent, the Irish government will process the request more quickly than if it is not urgent. If necessary, urgent requests can be processed in a matter of days.

5. In addition, the Criminal Justice (Mutual Assistance) Act, 2008, mandates procedures to ensure that evidence (most often bank accounts but also digital evidence) sought by an MLAT request is not destroyed or altered while the request is being processed. Where a foreign government requests that Ireland preserve (or "freeze") digital evidence located in Ireland, the Irish Department of Justice and Equality (acting as Ireland's Central Authority) can apply to the Irish High Court for a freezing cooperation order. This freezing cooperation order prohibits any person with possession of the evidence from altering or destroying it, and may also authorize the An Garda Síochána—Ireland's national police service—to seize property subject to the order to prevent it from being removed, altered, or destroyed.

Ireland generally processes requests for freezing cooperation orders within 24 hours from when they are made.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on 23rd July 2014.

Signed: /s/ MICHAEL MCDOWELL
MICHAEL MCDOWELL

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

No. 13 MJ 2814

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

July 31, 2014
10:45 a.m.

TRANSCRIPT, BEFORE THE HONORABLE LORETTA A. PRESKA, UNITED STATES DISTRICT JUDGE

APPEARANCES:

PREET BHARARA
United States Attorney for the
Southern District of New York

JUSTIN ANDERSON

SERRIN TURNER
Assistant United States Attorneys

ORRICK, HERRINGTON & SUTCLIFFE
Attorneys for Microsoft

E. JOSHUA ROSENKRANZ

ROBERT E. LOEB

BRIAN P. GOLDMAN

PETRILLO KLEIN & BOXER
Attorneys for Microsoft

GUY PETRILLO

COVINGTON & BURLING
Attorneys for Microsoft

JAMES GARLAND

NANCY KESTENBAUM

ZWILLGEN
Attorneys for Apple, Inc. and Cisco

MARC J. ZWILLINGER

STEPTOE & JOHNSON
Attorneys for Verizon Communications Inc.

MICHAEL A. VASTIS

SIDLEY AUSTIN
Attorneys for AT&T CORP.

ALAN C. RAUL

* * * * *

[28] indicate that Congress thought it was local. So the first version of ECPA incorporated Rule 41 hook, line, and sinker. Rule 41 in almost every sentence says "in this district." "Property in this district." It says it over and over again. That changed in 2001 with a statute that was called National Service of Process, that the legislative history described as a statute that was designed to break down district geographic boundaries and instead allow for service, "anywhere in the United States."

It is inconceivable that the Congress that first adopted the Rule 41 territorial limitations, and then expanded it to the nation, without ever saying it, was actually expanding the power of the government to conscript a private party to conduct a search that is outside the United States.

THE COURT: But they had done it for years under the Bank of Nova Scotia doctrine, using words just like the words that were used in the statute when it was passed about disclosure.

MR. ROSENKRANZ: Under the Bank of Nova Scotia doctrine, yes. But only as to documents that are the company's own records. I mean, Bank of Nova Scotia and Marc Rich did not overrule the preexisting law that says that when you are talking about records of other people, the government needs a search warrant, which I grant you they got, but the reason they got it is because this is a search and seizure. The warrant [29] protects U.S. citizens. But when you do the search and seizure in another country, it is fine for us to say that those people's privacy is protected. But Morrison says we ask whether the other country would be offended by the extension of U.S. law enforcement authority in the incursion on their sovereignty. And the answer is yes, they would be. Just like we would be if China or Russia or the United Arab Emirates did it to us.

THE COURT: Thank you.

Mr. Turner, counsel says that essentially that you should be using the MLAT procedure rather than doing

this. So essentially what is your response to the offense that the foreign sovereign would take at this sort of disclosure?

MR. TURNER: Your Honor, we don't need to go to a foreign country to get the records. The provider is right here. The provider is 10 feet away from me. The provider has control over the records. We can get them easily with domestic process. In that sort of circumstance, why would we go through all the extra hoops that are entailed in an MLAT? There is no reason to deal with the delays and complications that can certainly accompany an MLAT. I know Microsoft wants to push back and make it out as if the government can easily get records under an MLAT, but life is not that simple.

THE COURT: Of course Mr. DeMarco's affidavit is nothing other than fabulous.

[30]

MR. TURNER: Even Mr. DeMarco admits that foreign law enforcement authorities have their own priorities and they have to fit MLATs in with those priorities. It totally depends on the country you're dealing with. And of course, many countries don't even have MLATs to start with, and Microsoft has never answered that problem. What do we do if there is no MLAT? I guess we're just out of luck and can't get these records, even though there is an employee of Microsoft right here in the United States who can access those records on a keyboard just as if they were on a server under his desk and produce those records to us.

It is absurd. The potentials for abuse under that sort of system are enormous.

THE COURT: The practicalities aren't really the province here either. Isn't that something for Congress?

MR. TURNER: I think they are, your Honor. It is inconceivable that Congress would have intended these sorts of practical problems to result.

THE COURT: Counsel says that Congress could not have foreseen cloud computing, which is probably true.

MR. TURNER: I think, for example, the 2001 amendment showed that it was already aware of the issue of data location not being relevant.

The statute says that the government can get one of these orders from a judge who either is in the same district [31] that the data is located in or that the ISP is located in or that just has jurisdiction over the offense.

That in itself is good evidence that Congress understood that the government's need for this data should not be limited by sort of physical issues about where the data is stored.

It didn't want the government to have to go to another district to get the records. Why would it want to force the government to go to another country to get the records when all it has to do is obtain a warrant from a judge in the district where the offense is being investigated? And that warrant can be faxed, e-mailed, transmitted to the provider. They send back the records just like with a subpoena. This is nothing new. This is how the statute has worked for the past 30 years.

So, just going back to the MLAT point and this issue about retaliation by other countries. Microsoft can't

point to any abuses of privacy here, and they've admitted here today they don't have an issue with privacy, that the warrant takes care of any privacy interests.

So what they do is they conjure up speculative abuses by other countries. Now you are going to have other countries getting warrants to search members of Congress e-mail accounts, and New York Times reporter accounts. Completely speculative.

At the end of the day what other countries can do or will do under their legal systems is not at issue. What is at [32] issue are the rules of our legal system. The test is control, not location, and this has been the rule for decades. And the possibility of retaliation, I suppose, has been a possibility for decades.

You can say the same with bank records under BNS. Now other countries are going to get into members of Congress bank records. That possibility, to the extent it is a significant possibility, is a diplomatic issue for the political branches to deal with. It is not a valid basis for Microsoft to contest the warrant.

THE COURT: What do you say to counsel's suggestion about the cases you just mentioned to us, that in those cases, the customer, if you will, had not entrusted the content, essentially, to the holder, the possessor of the documents.

MR. TURNER: First of all, your Honor, I just say in terms of not citing cases before, it is because Microsoft has raised this argument anew in its reply brief. Their position has been in search of a theory throughout and the theory keeps changing.

As to your Honor's question, it is wrong. For example, just another case, U.S. v. Re, 313 F. Supp. 442. Another accountant case where it was the correspondence and other papers turned over to the accountant. The Court found, quote, that these papers were clearly the property of the clients. Nonetheless, it found it was proper to get them with [33] a subpoena.

* * * * *

[51] * * *

The difference between Microsoft doing it versus the government's doing it. ECPA I believe authorizes the government to do it in our place. To sit at the point of where the Microsoft employee is sitting. 2703(g) says that the government official need not be there. I think the government would agree that if a DEA agent is sitting at that terminal, then it is the government doing the search. And the government can't just substitute a private party under legal compulsion to perform that search. The government doesn't get to say just because we got someone else to do it, we're sort of scot-free and have no responsibility for the search.

And then the final point on the government's argument that it is just speculation as to whether foreign governments will be up in arms about the incursion on their sovereignty. It isn't speculation. The European Commissioner of Justice, Reding, we submitted a letter from her expressing outrage at the incursion on their sovereignty.

And I would, in terms of speculation, I would just punctuate the point by mentioning to the Court that just

this week, China served on Microsoft—excuse me. China appeared in Microsoft's offices in four locations in China to conduct a law enforcement search and seizure. They took our servers, okay, that's within their domain. They then demanded a password to seek e-mail information in the United States. Now, [52] the e-mail information was information of our own employees. But the government's point that there is no difference between correspondence that is simply our own documents versus correspondence that we are protecting on behalf of others means that tomorrow, China can do the same thing, and seize e-mail content from a server in China in the United States, and the government is saying—we know they would be outraged if China did it. The government's position means when China or Russia or one of these other countries does that next week, we have no claim that this infringes on our sovereignty. We have no argument that this was a search and seizure that occurs here. Because everything occurred in China and they just got a Microsoft employee in China to search its own business records over which it had possession and control.

That is a very, very dangerous principle that the government is articulating. It is dangerous—other countries view it as dangerous when they're talking about the United States. We view it as dangerous for sure when we're talking about our countries.

And an opinion from this Court saying that what the government did here is just fine because it is not an incursion on foreign sovereignty will be used by the coun-

tries that do this as Exhibit A that the government cannot possibly complain because one of the most respected judges in the United States says it is perfectly fine.

[53]

THE COURT: Oh, counsel, you say that to all the girls.

MR. ROSENKRANZ: I meant to say "the most respected."

THE COURT: Mr. Turner, what do you say to that? It's pretty scary.

MR. TURNER: First of all, your Honor, it sounds like a diplomatic issue to me. Again, it is not a basis for resisting a Congressionally authorized warrant directing Microsoft here. Other countries are going to do what other countries are going to do. We already have, like the government pointed to before, the Restatement, which already announces that this is recognized law in the U.S. That we can issue compulsory process to persons, companies here, and if they have the responsive records abroad, they have to produce them. So that's already embedded in the law. Again, it is nothing new. As I pointed before, the possibility of retaliation of some sort has been latent in that as well.

But again, to the extent that there are concerns about what other countries do in this area, obviously this is an emerging area of the law. That is something for the Executive to pursue through political and diplomatic channels. But it is not a valid basis for Microsoft to ask this Court to ignore the plain terms of the statute here,

which say that we can get an order and a warrant requiring them to disclose records based on probable cause. That's what we did. That's what any civil [54] libertarian would want to us do when the government needs communications like this.

We did it. The statute says the next step is Microsoft has to produce the records.

Microsoft has raised the issue of what about Ireland's concern here. First of all, I would just point out we are not talking necessarily about an Irish user. We are talking about data on an Irish server. The location of data is by no means a reliable proxy for the location of the user.

Under BNS, the only time you get into that kind of analysis, what about Ireland's concerns, is if there is a genuine conflict of law between the two countries. And here Microsoft has had every opportunity to assert that here, and has not been able to point to any specific provision of Irish law that in any way forbids it from handing the data over.

So, the sort of interest that Microsoft points to, the Court could in some other case, perhaps, take into account. But there is no need to do so here. Because there is no genuine conflict of law.

THE COURT: Thank you. Mr. Rosenkranz, did you want to end with anything?

MR. ROSENKRANZ: Yes. Please, your Honor. So, first, this is a diplomatic problem, to be sure. It is

especially a diplomatic problem when you take the Executive out of the picture, and posit that Congress authorized a sheriff's deputy * * * .

* * * * *

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

Docket No. 14-2985-cv

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORP.

MICROSOFT CORPORATION, PLAINTIFF

v.

UNITED STATES OF AMERICA, DEFENDANT

Sept. 9, 2015
10:27 a.m.

TRANSCRIPT OF HEARING

Before: HON. GERALD E. LYNCH, HON. SUSAN L. CARNEY, HON. VICTOR BOLDEN

APPEARANCES:

ORRICK, HERRINGTON & SUTCLIFFE LLP
Attorneys for Microsoft Corporation
51 West 52nd Street
New York, New York 10019

BY: E. JOSHUA ROSENKRANZ, ESQ.
(jrosenkranz@orrick.com)

U.S. DEPARTMENT OF JUSTICE
UNITED STATES ATTORNEY'S OFFICE
SOUTHERN DISTRICT OF NEW YORK
Attorneys for UNITED STATES OF AMERICA
One St. Andrew's Plaza
New York, New York 10007

BY: JUSTIN ANDERSON, ESQ.
(justin.anderson@usdoj.gov)

[3]

MR. ROSENCRANZ: Good morning, your Honors. May it please the court, Josh Rosencranz representing Microsoft.

Your Honors, the Stored Communications Act does not extend to electronic communications stored outside the United States because Congress never said that it should.

JUDGE LYNCH: Does that mean that Microsoft would be permitted to sell the contents of stored communications stored in Ireland to the National Enquirer if it chose to, at least as far as American law is concerned?

MR. ROSENCRANZ: As far as American law is concerned, yes.

JUDGE LYNCH: So if we found another country to store the stuff in, the communications in, that did not have the EU's protections, despite the fact that you're a United States corporation subject to, otherwise subject to American law, your position [4] is that you have an absolute right to disclose those communications, as far as American law is concerned, to anyone?

MR. ROSENCRANZ: As far as American law is concerned.

JUDGE LYNCH: As far as American law is concerned.

MR. ROSENCRANZ: Yes, your Honor.

But to be clear, Microsoft and any major international provider of email service does not store communications in any country that does not have robust protections.

JUDGE LYNCH: But you have the choice to, right?

MR. ROSENCRANZ: We do indeed.

JUDGE LYNCH: Under the agreement you make with your customers, you have the right to store those communications anywhere in the world that you choose, including Redmond, Washington, where they would be subject to American law, including [5] Ireland, where they would be subject to EU law. And including some island nation state with no protections for anybody, if you so chose.

MR. ROSENCRANZ: If we made that business decision, yes. And our consumer base would evaporate.

I want to underscore here, your Honor, there are two visions—

JUDGE LYNCH: It's just a little odd that you're here defending rights of privacy, in a certain way, at least that's the rhetoric that's in the brief, and yet what you're saying is that the American law that prohibits, except under controlled conditions pursuant to various

kinds of protections, protects the stored communications against disclosure, does not apply to you if you find another country to stash the stored records in. That's your position, is it not?

MR. ROSENCRANZ: That is our position, because Congress, when it [6] was protecting the storage of communications, was protecting them in the place of storage. It was not, and at the time, no—

* * * * *

[10]

MR. ROSENCRANZ: 2703 is a prohibition against—excuse me, 2703 is a permission to disclose that carves out an exception to the rule against disclosure in electronic communications.

JUDGE LYNCH: Right.

MR. ROSENCRANZ: Of electronic communications in electronic storage.

The common theme is the storage, your Honor. And the government, I understand you're pointing out that there is a gap. This is an anachronistic statute. There will be a gap regardless of what you identify as the focus of Congressional concern.

The government says—

JUDGE CARNEY: Were U.S. service providers storing or operating in any significant way outside of the United States in 1986 when the Stored Communication Act was passed?

MR. ROSENCRANZ: No, your Honor, they were not.

* * * * *

[53] * * *

JUDGE CARNEY: So what text in the Stored Communications Act do you point to to support your assertion that this is, Congress intended extraterritorial application?

MR. ANDERSON: There is no extraterritorial application here at all.

JUDGE CARNEY: Because the point of access is here?

MR. ANDERSON: Right, the disclosure is here.

What this is concerned about, 801, 02, and 2703 is disclosure. [54] Involuntary disclosure, voluntary disclosure, government ordered disclosure. And where does the disclosure take place, is here.

In fact, Microsoft hangs its hat on the statutory term "electronic storage." And we assume it knows what it means by that—

JUDGE CARNEY: Therefore a German court requiring disclosure of a provider in Germany, regardless of where its servers are kept or who it's providing service to, can require the disclosure to happen there and U.S. customers or users can be effected but it should be of no concern to us. Is that right?

MR. ANDERSON: No, it should be of some concern.

But the fact is that under international law, this is the norm. The norm is that sovereigns, having jurisdiction over entity and people before them, can compel those entities and individuals to produce materials.

[55]

Now, of course there is a balancing that occurs in the United States, as the court is aware, from Linde against Arab Bank, that there are factors that District judges and of course the Court of Appeals can weigh before ordering the production of materials, where there are bona fide foreign, internet foreign laws that prohibit the disclosure.

JUDGE LYNCH: That raises the question, has there been a comity analysis of any sort performed explicitly by the District Court in this case?

MR. ANDERSON: Repeatedly, the government has invited Microsoft to identify what law it would be violating, what prohibition it bars the production of these records. And it has come up with nothing. At each stage in this litigation it has pointed to different EU politicians or statements of parties that have some interest in this case.

* * * * *

[59]

MR. ANDERSON: * * *

But they've conceded they have that custody and control. For their own business purposes they choose to be able to access data from in the United States wherever in the world it might be stored. And that is the

type of custody and control that this court determined in the Citibank case from the late '50s is required to order an entity to produce those materials.

JUDGE LYNCH: And we don't know whether the person whose records the government—whose communications the government was seeking is a United States person or not, in this record?

MR. ANDERSON: That's right.

JUDGE LYNCH: And so from the government's position it doesn't matter. We should assume for purposes of this issue, from the government's [60] vantage point, that this is an Irish national whose records are being sought from the servers in Ireland?

MR. ANDERSON: We could assume, if that were the case.

JUDGE LYNCH: If that were the case it wouldn't change the government's analysis at all?

MR. ANDERSON: It wouldn't change the government's analysis.

JUDGE LYNCH: Just as apparently, I guess I'll ask Mr. Rosencranz this, I don't think it affects Microsoft's analysis if we knew the person wasn't American who had made a contract with Microsoft and they decided jointly to store the communications outside the borders, none of that—we don't know which it is, and it doesn't matter?

MR. ANDERSON: Exactly right, judge.

And it's also highly unlikely that in a narcotics investigation like this one, the court is aware, that at [61] the

time the court is issuing subpoenas, orders, warrants, it has any idea about the nationality, this is an international case, the geographic location of any of these people. It's only far later in these types of cases where we would even know if it was a U.S. citizen or foreign national.

JUDGE LYNCH: I take it when the warrant was actually issued, based on the language of the warrant itself, and based on the record as far as I read it, the government was not issuing a warrant for documents stored in Ireland, it was obtaining from the court a warrant for documents in the custody and control of Microsoft. And for all you knew, or for all the warrant application and the warrant reveal, the records might well have been in the United States?

MR. ANDERSON: That's right.

And that's also why this is not an extraterritorial application of [62] anything. The government is indifferent to where Microsoft might have to go to gather these materials.

JUDGE LYNCH: This is a larger question about the scope of Morrison that I found perplexing in other contexts as well, as to identifying what counts as an extraterritorial application of a statute.

It's easy when you're talking about a criminal prohibition on behavior, if you're prohibiting behavior that occurs here, it's not extraterritorial, if you're prohibiting behavior that occurs in Italy, that's extraterritorial. But it gets murkier in situations like this, as you point out, the disclosure is made in the United States, the contract may well be made in the United States, I don't know how this one—how, you know, the back and forth

went to establish this account. The documents are stored in Ireland.

In this case, I take it the [63] record reflects that Microsoft could have put them anywhere, but at the same time it also reflects that under the normal practice a person indicating that he was from Ireland might assume that they were going to be kept in Ireland, though they couldn't guarantee it.

MR. ANDERSON: It's not clear that that's public knowledge.

JUDGE LYNCH: There is a lot of variations about what's occurring there and what's occurring here. And it's a nice slogan to say there shan't be any extraterritorial application.

I take it the government's not exactly taking issue with that proposition that the Stored Communications Act does not apply extraterritorially, at least for purposes of this case, but it is suggesting that this application is not extraterritorial, that's the principal argument?

MR. ANDERSON: Exactly right, [64] Judge. That that presumption applies to all statutes.

But here, if we look at what the focus of this statute is, which is what Morrison requires the court to do, the focus of this statute is disclosure. And it's this disclosure—

JUDGE LYNCH: Well, does that mean that it's the government's position as well that if Microsoft stores its communications in Germany, it could sell those communications to the German National Enquirer and

not violate the Stored Communications Act because the disclosure would take place abroad?

MR. ANDERSON: That very well might be the conclusion of a court.

In fact, it was the conclusion of the Northern District of California when Yahoo users, whose content was disclosed to the Chinese government, brought an action under this statute, and the court said this doesn't apply [65] to that disclosure, the disclosure took place in China, by a Yahoo subsidiary there.

So it might very well be the case. That was a decision at the Trial Court stage, and there hasn't been a lot of law in this area. That an American user might not have a right to complain under this statute if the data is disclosed overseas.

But what we're talking about here is U.S. law enforcement requiring Microsoft, which is subject to U.S.—the jurisdiction of U.S. courts, to produce records in the United States. The warrant itself doesn't say go to Ireland and retrieve these records. The warrant doesn't care where the records are.

JUDGE CARNEY: And what indication in the statute is there that Congress didn't care either?

MR. ANDERSON: There is no indication in the statute that Congress was at all concerned with [66] storage.

* * * * *

[70]

MR. ANDERSON: * * * And then we have the mandatory disclosures, which pertains to how the government can obtain this information [71] from service providers.

So the idea that this is about storage, the word "storage," or the word "stored" is in there.

JUDGE LYNCH: It's about things that are stored. It's about things that are stored. And it regulates under what circumstances those things may be disclosed and not disclosed?

MR. ANDERSON: Correct.

And that's the focus here is on disclosure and privacy, not the regulation of storage. Because the act has nothing to say about how and where and whether these items are stored. It's all about how they're made private or how they're disclosed to either the public or the government. And what requirements must be held.

JUDGE LYNCH: You know, I'm a little hesitant to keep pushing the government to take positions on things that aren't here in the statute, and I don't know to what extent you are [72] authorized to take positions on all of those. But the implications of what we do here are obviously broad.

So Mr. Rosencranz suggested that the Irish government would not have access to these communications if it sought, under its own law and its own law enforcement interests, to get them in Ireland, because the prohibition on disclosure would cover that situation.

Am I to understand that the government's position, and this goes back to whether there is an extraterritorial application to the basic prohibition in 2702, the government's position is no problem, because the disclosure that is regulated is disclosure in the United States, and disclosure abroad is fine under whatever rules apply? So if there is a country where there are—it's the wild west, Microsoft can do whatever it wants with anything that stores over there, or that it could disclose—you could take records [73] that are in Redmond or New York City, send them over to another storage facility in, you know, some briefcase bank country or other which has no regulations, and then disclose to the National Enquirer what the communications are.

If it's in the EU where that sort of thing wouldn't be allowed, but there, I'm guessing, are some sort of law enforcement exceptions like the ones here, it could comply with orders from the Irish courts to disclose things in Ireland, and that would not violate this statute. Is that the government's position?

I'm just trying to understand it, because Mr. Rosencranz is making an argument that has some force that if we apply this statute in its broadest terms to anything that takes place all over the world, it would have, in his view, the effect of regulating what foreign law enforcement could do, and that would [74] be weird.

MR. ANDERSON: Right.

And so if Microsoft chose to store all of its emails in the Cayman Islands or some jurisdiction it found that would be beyond EMLAT, wouldn't comply with our subpoenas, or warrants or any other type of voluntary

submission of those materials, and if it chose to set its server there and the government of the Cayman Islands said, well, you have custody and control over all of these records, and under our law that means you must produce them to us, Microsoft cannot come to the United States and complain, we're prohibited by this statute that governs domestic disclosures.

This is all about the U.S. Government compelling an entity that's subject to a U.S. court to produce records here.

JUDGE LYNCH: I take it that suggests that the government actually [75] agrees that there shall not be extraterritorial application of the Stored Communications Act, it's just—what this dispute is about is about the focus of the statute and what counts as an extraterritorial application of the statute?

MR. ANDERSON: That's right, Judge.

And the focus here, as described in each of these sections, most particularly 2703, which pertains to disclosure, is about the disclosure of records. And if the disclosure occurs in Ireland, you know, in the case where we don't have any additional facts, it would seem that this statute would have nothing to do with that act. It doesn't regulate that.

JUDGE LYNCH: So both sides are in agreement that there may not be as much protection of the privacy of one's electronic communications as the electronic communicator might like. Based on this statute.

[76]

Because either way you look at it, there will be—there is considerable latitude on the part of service providers to set things up in such a way that they can do whatever they want with the communications if they do it abroad, or it's just a question of whether they make the disclosures abroad or whether they store the records abroad?

MR. ANDERSON: That's right, Judge. And that's why I mentioned the case from the Northern District of California that dealt with the Yahoo example.

But the point here is that if the items are stored in the United States, the users, and if the government seeks to obtain them, Congress has imposed the highest standard to protect privacy.

It's really the gold standard. It is the warrant, that's the time tested way of protecting the legitimate privacy interests of [77] individuals.

* * * * *

[88] * * *

JUDGE LYNCH: Can I just come back to one thing Mr. Anderson argued, I want to know if you agree with it.

He said that throughout this litigation Microsoft has never identified a specific EU law that would prohibit the disclosure that the government seeks, unlike in, for example, Mark Rich where there were specific Swiss banking privacy laws that Mark Rich and company argued precluded the production of the financial records that were sought.

Is that the case? Is there some EU law that prohibits the disclosure that the government seeks in this [89] case?

MR. ROSENCRANZ: Well, your Honor, we are certainly very concerned about that. I will not stand up here in a public forum and tell the court that if we comply with a court order here we are violating foreign law.

JUDGE LYNCH: Fair enough. Let me then rephrase the question.

Is there some specific EU law that you could point us to that we—that you are concerned about and that we should be concerned about, preserving the fact that you reserve the right to argue, if it comes to that, and in whatever EU jurisdiction that you wouldn't be violating that law. But what are the laws we should be looking to that might create this kind of conflict of jurisdictions?

MR. ROSENCRANZ: So let me point to two sources, and then we identify more in the digital whites, Ireland brief identifies more as well.

So the first place to look is [90] the declaration on page A-116 of the Attorney General of Ireland. So paragraph 10, for example. He says—that is the former Attorney General of Ireland, excuse me, "absent certain particular exceptions, disclosure to a third party of such data, that is data stored and processed in Ireland, is only lawful pursuant to orders made by the Irish courts."

He goes on, second major source, it's cited in our reply brief, it's the European Data Protection Authority's joint statement, it is the European Privacy Regulator's

statement of what the law is. "As a rule, a public authority in a nonEU company should not have unrestricted direct access to the data of individuals processed under EU jurisdiction. Foreign requests must not be served directly to companies under EU jurisdiction."

And we cite a few more. But there they are basically along those [91] lines. And I have to underscore—

JUDGE LYNCH: That declaration from the expert on Irish law and that statement from the EU regulators, they cite to sources of law that we could then look at the original?

MR. ROSENCRANZ: Yes, your Honor.

JUDGE LYNCH: That's where I should be looking.

MR. ROSENCRANZ: They cite to the Irish act, Data Protection Acts of 1998 and 2003.

But I also want to underscore that under Morrison, the existence of an actual conflict with foreign law is not relevant.

* * * * *